The new EU General Data Protection Regulation (GDPR) in medical data and clinical research

Vretta Maria

SCHOOL OF ECONOMICS, BUSINESS ADMINISTRATION & LEGAL STUDIES

A thesis submitted for the degree of

Master of Science (MSc) in Bioeconomy Law, Regulation and Management

November 2018
Thessaloniki – Greece

Student Name:	Maria Vretta
SID:	4402170008
Supervisor:	Prof. Takis Vidalis

I hereby declare that the work submitted is mine and that where I have made use of another's work; I have attributed the source(s) according to the Regulations set in the Student's Handbook.

November 2018
Thessaloniki - Greece

Abstract

This dissertation was written as part of the MSc in Bioeconomy Law, Regulation and Management at the International Hellenic University.

The purpose of my research is to conduct an extensive legal analysis of the existing legal framework on data protection in medical data and clinical research. The recent General Data Protection Regulation (EU) 2016/679,"GDPR", enhances the fundamental rights of individuals in the field of data protection. Medical data specifically, as they refer to a person's health are sensitive data that require additional protection and careful handling. This is the case in clinical research also. This analysis includes European Law, namely the Data Protection Directive, the GDPR, Convention 108, the European Convention on Human Rights (ECHR) and Guidelines on the Protection of Individuals with regard to the Processing of medical data and clinical research data.

I would like to express my gratitude to my supervisor Professor Dr. Vidalis, for the support and the valuable guidance. His expertise, understanding and patience contributed considerably to my dissertation thesis. Moreover, I would like to thank Dr. Savvas Gennitsaris for his support during my studies for this MSc.

Finally, I would like to express my sincere thanks to all people around me that motivated and encouraged me during this experience.

Keywords: GDPR, medical data, protection, clinical research, EU

Vretta Maria
30.11.2018

Preface

The basis for this research originally stemmed from my passion in EU law and the protection of human rights. As the world moves further into the digital age, generating vast amounts of data and born digital content, there will be a greater need to analyse the legal framework in data protection and the challenges that arise. How can individuals' rights be adequately protected in the current legislation? How do the EU and CoE data protection framework address the data protection in sensitive data? Which fundamental rights issues do the processing of sensitive data may create?

I hope you enjoy your reading.

Vretta Maria

Contents

List of Abbreviations

Abbreviations	Explanation
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPD	Data Protection Directive
DIA	Data Impact Assessment
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
EHR	Electronic Health Records
EU	European Union
GDPR	General Data Protection Regulation
iPSC	Induced pluripotent stem cells
OECD	Organisation for Economic Co-operation and Development
SHA	Safe Harbour Agreement
TFEU	Treaty on the functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations
WP29	Article 29 Working Party

Introduction

The EU's General Data Protection Regulation (EU) 2016/679 aims to extend data protection to the era of big data and cloud computing, ensuring that data protection is a fundamental right that will be regulated consistently throughout Europe. Big data is a term used to refer to the study and applications of data sets that are too complex for traditional data-processing application software. Big data include capturing data, data storage, data analysis, search, sharing, transfer, visualization, querying, updating, information privacy and data source[1]. Any company that serves European customers and collects their data should comply with this Regulation, even if it is based in a non-European country. The new GDPR is the biggest change in data protection legislation over the last 20 years. The new Regulation present clear rules tailored to the digital age to provide strong protection. It imposes a higher standard of protection for the processing of medical data. New technologies facilitate the digitalization of medical information in the form mostly of Electronic Health Records. While, digitalization of Health Records is important for improving and revolutionizing healthcare services the use of Electronic Health Records carries enormous risks for private and security. Medical data is subject to stricter data-processing regime than non-sensitive data. In the field of clinical research, the new EU General Data Protection Regulation, while aiming to provide better safeguards for individuals' personal data may also have significant implications for data protection practices of researchers, industry, and Biobanks around the world. This dissertation thesis aims to provide an overview of the new concepts the new General Data Protection Regulation presents and to scrutinize the new framework that the Regulation forms in the field of medical data and clinical research, along with the repercussions that might occur.

Brief History of Data Protection in Europe

World War II, which ended in 1945, besides the tremendous social and economic impacts, led governments, especially in Europe, to realize the necessity of

[1] Hilbert, M., & López, P. (2011). "The World's Technological Capacity to Store, Communicate, and Compute Information". *Science*, 332(6025), 60 –65.

implementing laws to protect personal data to prevent similar atrocities. Once Hitler's Nazi regime came to power in 1933, the government began to gather card catalogues classifying political and racial enemies of the German. One of the methods used to identify citizens of Jewish race or descent was the "National Census". This Census required all citizens to declare both their religious beliefs and race.

In 1948, the United Nations' *Universal Declaration of Human Rights ("UDHR")* was adopted, and Article 12 of the UDHR declared that "[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[2]

Following the UDHR, Europe responded in the need of protecting human rights, personal data and privacy with the *European Convention on Human Rights (ECHR)*. ECHR was drafted in 1950 by the newly formed Council of Europe and was entered into force on 3 September 1953. Specifically, Article 8 provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society"[3]. Eight fundamental principles of data protection were established by the Organisation for Economic Co-operation and Development ("OECD") in 1980. The OECD's data protection principles are outlined in Part II of the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[4]. These principles, revised in 2013, reverberate in ensuing data protection legislation that was adopted in different countries around the world[5]. Hence, the study of these principles became a useful introduction into understanding the European regime. In 1981, the Council of Europe adopts the Data Protection Convention, known as *Treaty (Convention) 108*, rendering the right to privacy a legal imperative.

[2] http://www.un.org/en/documents/udhr/
[3] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005
[4] https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
[5] Colin J. Bennett, (1992), "REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES:, *Cornell University Press*, Ithaca and London

In 1983, the German Constitutional Court summarized the value concept of data protection with a fundamental decision[6]. The "Bundeserfassungsgericht", in its landmark decision on the Volkszählungsgesetz (VolkszählungsG) [Law on the General Census][7] explained the notion of data protection as the right of informational self-determination, which can be defined in practice as the desire of individuals for assurances that custodians of their personal data will comply with fair information practices[8]

In 1995, the European Commission (EC) promulgated a new "Directive" which was now binding upon EU member states. The *Data Protection Directive 95/46/EC*[9] obliged each EU member state to implement privacy laws that are "equivalent" to one another. It, furthermore, required that data could only be exported to third party countries that could guarantee "an adequate level of protection" for European citizens' data through their domestic laws or through international commitments. The Directive was implemented in 1998 including Article 29 which presented the composition and purpose of the Article 29 Working Party (WP29).

In 2002 EU adopts *Privacy and Electronic Communications Directive 2002/58/EC* which regulated key subjects such as confidentiality of information, traffic data, spam and cookies. *Directive 2006/24/EC* of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC" was adopted in order to regulate telecommunications data which member states had to store them for a minimum of 6 months and at most 24 months. Furthermore, police and security agencies had the right to request access to IP address and time of use of every email, phone call and text message sent or received. However, this Directive was declared invalid by the European Court of Justice because it violated the EU Charter of Fundamental Rights on 8 April 2014.

---

[6] Burkert, H. (2000), "Privacy Data Protection. A German/European Perspective" In C. Engel & K. H. Keller (ed.), *Governance of Global Networks in the Light of Differing Local Values* (pp. 43--70). Nomos Verlagsgesellschaft.

[7] Germany/Bundesverfassungsgericht/Judgment of 15 December 1983 ('Volkszählungsurteil') [Judgement on the Census], BVerfGE 65, 1

[8] David H. Flaherty, (1991) "On the Utility of Constitutional Rights to Privacy and Data Protection" 41 Cas. W. Res. L. Rev. 831 Available at: http://scholarlycommons.law.case.edu/caselrev/vol41/iss3/14

[9] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046

Directive 2009/136 amended Directive 2002/58/EC mainly regarding to cookies, where it introduced the requirement of prior consent. On 2013 EU issues the *Regulation 611/2013* on the measures applicable to the notifications of personal data breaches under Directive 2002/58/EC.

2014 was an important milestone in data protection since the Court of Justice decides that data about individuals held by Google must be deleted on request. Anyone has the right to ask search engines to remove results from queries that include their name. The concept of this ruling became known as the "right to be forgotten"[10].

In 2016, after approximately four years of discussions The General Data Protection Regulation (EU) 2016/679[11] was adopted superseding the Data Protection Directive 95/46/EC.

[10] Google Spain SL and Google Inc. against Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case number C-293/12". Court of Justice of the European Union. 8 April 2014. http://curia.europa.eu

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),

1 Legal Framework

Legal instruments developed by the Council of Europe and the EU often converge in the protection of privacy and personal data but they as well present differences in certain aspects.

1.1 Main Legal Instruments

Relating to the Council of Europe legal instruments is the Article 8 of the *European Convention on Human Rights* which protects the rights to privacy and personal data and additionally guarantees the right to respect for private and family life, home and correspondence[12]. Another key binding instrument is the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,* known as *Convention 108*.

In EU primary law Article 16 of the Treaty on the functioning of the European Union (TFEU) contains a general EU competence to legislate on data protection issues[13]. The Charter of Fundamental Rights (EU Charter) in articles 7 and 8 acknowledges the respect for private life and the right to data protection. The principal secondary EU law instrument until May 2018 was the Data Protection Directive, which was replaced by the General Data Protection Regulation.

1.2 Council of Europe legal framework

ECHR

The *European Convention on Human Rights (ECHR)*[14] was drafted in 1950 by the Council of Europe and entered into force in 1953. All Council of Europe member states, which now are 47, are party to the Convention including all the EU Member States.

[12] Convention for the Protection of Human Rights and Fundamental Freedoms,(1950) https://www.coe.int

[13] Consolidated version of the Treaty on the Functioning of the European Union,(2008) *Official Journal C 326 , https://eur-lex.europa.eu*

[14] European Convention on Human Rights, amended 2010, https://www.echr.coe.int

The Convention established the European Court of Human Rights (ECtHR) that is why it is considered to be the most effective in terms of individual protection against human rights violations in Europe. Judgments finding violations are binding on the States concerned and they are obliged to conform to them. The Convention is applicable at a national level and it has been incorporated into the legislation of the States parties. All domestic courts must therefore apply the ECHR. The interpretations of the Convention provisions by the ECtHR are very significant because through these the protection of human rights and freedom evolves and strengths.

Article 8 of the ECHR guarantees the right to respect for private life, family life, home and correspondence. Its scope is very broad[15]. Nevertheless, the protection awarded by Article 8 ECHR is, however, limited. The rights protected in the 1st paragraph may be hindered from the conditions laid down in paragraph 2. European Court of Human rights has not yet defined in a precise way the notion "private life". In general, ECtHR in its jurisprudence has given a broad interpretation of article 8 which is in accordance with the nature of the Court as a living instrument; consequently it must take into consideration the constantly changing social, legal or technological conditions in order to be "practical" and "effective"[16]. In many cases though, ECtHR has given some examples of the protection that Article 8 of the ECHR provides, such as the mere storage of information about an individual private life[17], the surveillance on the workplace [18] and the surveillance and interception of phone and mail communication[19] among others.

However, there are limitations which are set by the 2nd paragraph of Article 8. There are, according to Article 8.2 cases where the public authorities can legally interfere with the rights set out in Article 8.1 under three conditions:

[15] Steven Greer , (1997)"The exceptions to Articles 8 to 11 of the European Convention on Human Rights", Council of Europe, Printed at the Council of Europe
[16] Tyrer v. the United Kingdom, (Application No. 5856/72), Judgement 1978,
[17] Leander v. Sweden,26 May 1987 (Application no. 9248/81),
[18] *Copland v. the United Kingdom* Application No. 62617/00, (Judgment 2007)
[19] Klass and others v. Germany, (Judgment 1978) *(Application No. 5029/71),*

a) The interferences must be in accordance with the law. "*The national law must be clear, foreseeable, and adequately accessible*"[20]. The law must be adequately clear in its provisions to provide any individual a sufficient precision of the conditions and circumstances in which the authorities are empowered to resort to any interference with an individual's right to private and family life, home and correspondence. Article 8.2 introduces the requirement of *foreseeability*. Laws with general content do not meet with this standard[21].

b) They must pursue one or more legitimate aims. Article 8.2 enumerates, with a limited list, the legitimate aims which may justify an infringement upon the rights protected in the first paragraph.

c) The restrictions must be "*necessary in a democratic society*". It is apparent, therefore, that the rights protected by Article 8.1 are not absolute and the ECtHR always examines if in a case the above conditions apply. To determine whether the impugned measures are "*necessary in a democratic society*", it is important that the reasons adduced to justify them are relevant and sufficient and the measures are proportionate to the legitimate aims pursued[22]. The proportionality of a general measure balances the interests of the Member State against the right of the applicant.

The primary purpose of Article 8 may involve the adoption of measures designed to secure respect for private life[23]. The affective enjoyment of the rights protected by the ECHR not only obliges the States to abstain from any interference but also to actively ensure the protection of these rights[24].

Certainly, States enjoy a certain margin of appreciation when implementing their positive obligations under Article 8. The breadth of that margin varies depending on whether an individual's existence or identity is at stake or whether the State is required to strike a balance involving opposite private and public interests or

[20] Silver and others v. the United Kingdom, (Judgement 1983) (Application No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75),

[21] Amann v. Switzerland , (Application No. 27798/95), (Judgement 1983)

[22] Z v. FINLAND, *(Application no. 22009/93),* (Judgement 19997)

[23] The principle was first set out in Case of Marckx v. Belgium, *(Application No.6833/74),*(Judgment *1979)*

[24] In the case of *K.U. v. Finland* (application No. 2872/02), the Court held unanimously that there had been a violation of Article 8 (right to respect for private and family life) of the European Convention on Human Rights concerning the Finnish authorities' failure to protect a child's right to respect for private life following an advertisement of a sexual nature being posted about him on an Internet dating site.

Convention rights. The margin of appreciation is particularly wider when there is no European consensus on issues with sensitive moral or ethical issues.

Convention 108

The Convention laid down basic principles for data protection, also referred to as the "*common core*" principles[25]. Notwithstanding, CoE regulations and in this case Convention 108 are addressed to states in line with the standards of international Conventions, implying a weaker binding nature[26].

Convention 108 protects persons against infringements of personal data during processing and seeks to regulate the Transborder flows of these data. It applies to all data processing by the public or the private sector. In addition, it outlaws the processing of "sensitive" data on an individual's race, politics, sexual life, health, religion or criminal record when the suitable safeguards by the law do not exist. Moreover, it enshrines the person's right to know what and how many data are stored about him or her and to correct them if it is needed and in addition offers a remedy if any of the previous elements are not respected. Transborder flows of personal data to States where legislation does not provide enough protection is restricted by the Convention. Security or defence may lead to limitations on the rights of the individuals. However, Convention 108 does not consider consent of the data subject as a legitimate ground for processing.

Currently, the Convention is undergoing a modernisation process. This process started in 2010 with CoE's regulators trying to ensure that the Modernized Convention will be in compliance and compatible with the new GDPR[27]. In September 2016, the CoE published a Draft Modernised Convention 108 that tries to complete these aims[28].

[25] Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (1981) ETS 108 (Explanatory Report to Convention 108)
[26] Jörg Plakiewicz, (2011), "Convention 108 as a global privacy standard?" International Data Protection Conference Budapest
[27] EU Agency for Fundamental Rights and Council of Europe, "Handbook on European data protection law" (2018 edition) (Luxembourg: Publications Office of the European Union.
[28] "Consolidated text of the modernisation proposals of Convention 108 finalised by the CAHDATA" (meeting of 15-16 June 2016 (Draft Modernised Convention 108)

In May 2018, the Committee of Ministers adopted a Protocol amending Convention 108[29].

1.3 EU legal framework

Charter of Fundamental Rights of the European Union

The Charter of Fundamental Rights of the European Union was proclaimed by EU in 2000. It sets out the full range of political, economic, civil and social rights of European citizens, through the synthesis of international obligations and constitutional traditions common to all Member States. The Charter became legally binding on EU Member States when the Treaty of Lisbon entered into force in December 2009. Article 51 of the Charter states that all Member States as well as EU institutions, when implementing EU law, must examine and guarantee all the rights of the Charter. Specifically, the rights to private and family life and data protection are protected by article 7 and 8 of the Convention.

The Charter must not be confused with the European Convention on Human Rights. Although some provisions are relating, the two operate within separate legal frameworks:

- The Charter of Fundamental Rights of the European Union was drafted by the EU and is interpreted by the Court of Justice of the European Union (CJEU).
- The European Convention on Human Rights, on the other hand, was drafted by the Council of Europe in Strasbourg and is interpreted by the European Court of Human Rights.
- Unlike the ECHR, the Charter of Fundamental Rights not only guarantees the respect for private and family life, but also establishes the right to data protection explicitly. Data protection, as a result, became a fundamental right in the EU law.

On the other hand, there are limitations to the fundamental rights in the Charter similar to the ECHR. Article 52.1 of the Charter enumerates the circumstances when limitations on the rights and freedoms protected by the Charter are admissible.

[29] Ad hoc Committee on Data Protection (CAHDATA), Protocol (CETS No. 223) amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CM(2018)2- final, 18 May 2018

Secondary law

Until 2018, under EU law, data protection was regulated primary by Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive, DPD). In 2018, the Directive was replaced by the General Data Protection Regulation (GDPR), which was adopted as part of the EU Data Protection Reform Package[30].

Furthermore, when balancing other legitimate interests there are more detailed data protection provisions that ensure clarity and consistency always alongside GDPR. Particularly, Directive 2002/58/EC regulates on the processing of personal data and the protections in the electronic communications sector and Directive 2000/31/EC sets up a framework on certain legal aspects of electronic commerce in the Internal Market and mere conduit.

In data protection framework Court of Justice of the European Union (CJEU) has jurisdiction to determine whether a Member State has fulfilled its obligations under Article 7 and 8 Charter of Fundamental Rights and to give preliminary rulings concerning the validity and interpretation of the Directive and the Regulation, in order to ensure its effectiveness and uniformity.

Soft law

Soft law refers to non-legally binding instruments such as opinions, recommendations, resolutions and declarations, codes of conduct, guidelines and communications. Although they do not have legally binding force they may set standards and are important in increasing the value of international agreements or other legally binding instruments.

Soft law constitutes declarations, resolutions of the Council of Europe's statutory organs such as the Parliamentary Assembly and the Committee of the Ministers. Also, opinions and studies of the European Commission for the Democracy

[30] Directive (EU) 2016/680, entered into force in 5 May 2018

through law (Venice Commission), which is the Council of Europe's advisory body on constitutional matters, are an example of soft law. In addition, soft law are opinions of the European Data Protection Supervisor, which is a supervisory authority devoted to protecting personal data and privacy.

Regarding European Union, in the protection of personal data, an important role played the opinions and recommendations of the Article 29 -Working Party[31], which was an advisory body, composed of representatives from the data protection authorities of the Member States of the EU, the European Data Protection Supervisor and a representative of the European Commission. As of 25 May 2018 the Article 29 Working Party ceased to exist and has been replaced by the European Data Protection Board (EDPB). It is composed of the head of each Data Protection Authority and of the European Data Protection Supervisor (EDPS) or their representatives. The European Commission takes part in the meetings of the EDPB without voting rights[32].

2 Privacy v. Data Protection

A first distinction between privacy and data protection lies in the scope and the limitations of both rights. The distinction is important in order to understand that not all situations covered by data protection law are covered by the right to privacy and vice versa. These rights are closely related, but they are not the same. In Opinion 4/2007 on Personal data of Article 29 Working Party there is a reference in the difference of the right to privacy and data protection: "*the Charter of Fundamental Rights of the European Union enshrines the protection of personal data in Article 8 as an autonomous right, separate and different from the right to private life referred to in Article 7*"[33]. Moreover, the jurisprudence of the European Court of Human rights and the Court of Justice of the European Union in many cases separated the function of

[31] The composition and purpose of Article 29 WP was set out in Article 29 of the Data Protection Directive.
[32] Articles 63 to 76 and Recitals 135 to 140 of the GDPR
[33] https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_en.pdf

these two rights, particularly with reference to the scope of both rights and their limitations[3435].

Scope and Limitations

"Private life" is a broad concept, which is constantly evolving. Although data protection right is also broad the right to privacy covers many other aspects in addition to the protection of personal information. Therefore it is much broader than the data protection right. The ECtHR has interpreted "private life" as a notion that includes the protection of personal data being defined as any information relating to an identified or identifiable individual[36]. A closer analysis, however, of the case law discloses that the ECtHR requires an additional element of privacy in order for personal information to be included in the scope of private life. This element may be the intrusive nature of the processing, because the processing may refer to medical or health data or data of vulnerable groups or the processing refers to a permanent or long-term period which is a breach of the right to privacy[37]

In the substantive scope **"**private life" does not necessarily include all information on identified or identifiable persons. The data protection right, on the other hand, does. It protects the processing of personal data relating to an identified or identifiable person despite the consequences this processing has on privacy. Even outside the privacy context the "*data protection right is a fundamental one and it aims at facilitating data processing and not forbidding it*"[38] .

In the personal scope, in principle, legal persons do not enjoy the right to data protection[39].The reasoning of CJEU behind this exclusion lies in Article 2(a) and Recital 2 of the Data Protection Directive(DPD), which limit data protection to natural persons,

---

[34] CJEU, Joined Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation v Council and Commission*, [2008] ECR I-6351, para. 285.
[35] CJEU, Case C-28/08 P Commission/Bavarian Lager [2010] ECR I–6055, para. 60
[36] CJEU, Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-11063, para. 52.
[37] ECtHR, *Rotaru v Romania* App no 28341/95, ECHR 2000-V, para. 44. In this case security services detained a file containing information of fifty years about the applicant's life. The ECtHR decided that the processing of information for such a long period of time falls within the scope of "private life".
[38] CASE C-101/01, Bodil Lindqvist JUDGMENT OF 6. 11. 2003 —
[39] CJEU, Joined Cases C–92/09 and C–93/09 *Volker und Markus Schecke and Eifert* (2010) ECR I-11063, para. 58, and Joined Cases C-465/00, C-138/01

although the Charter of Fundamental Rights grants to "everyone" privacy and data protection. In Recital 14 the new GDPR limits its protection to natural persons and does not cover the processing of personal data concerning legal persons, in particular undertakings established as legal persons or legal entities. This exclusion contains the name of the legal person, the form and the contact details of the legal person. There is a "grey zone" in the new GDPR because information that concerns legal persons may at the same time be personal data of a natural person, and vice versa In this dilemma, it would be instrumental to use the criteria of "purpose", "content" and "result" in evaluating whether or not GDPR should apply,[40]. Only ECtHR has recognized that legal persons have a right to privacy[41].

It must be underlined that even if a case does not concern processing of personal data it does not mean that it is not a breach to privacy and for that reason must be protected under Article 8 of ECHR. The same applies in cases where there is interference with the right to data protection but at the may not constitute a violation to private life. It is evident that the rights to privacy and to protection of personal data may sometimes overlap and the distinction between them is not always clear in practice.

There is, moreover, a difference between privacy and data protection with regard to permissible limitations. The right to privacy is not limited by any means, except when interference is justified under certain conditions.

In the same manner the right to protection of personal data which is protected explicitly by the EU Charter in Article 8.2 where the conditions of lawfulness of the processing are defined; fairly processing of data for specified purposes and on the basis of consent of the person or another legitimate basis provided for by the law. Article 52.1 of the Charter will cover the cases where the conditions of article 8.2 for the lawful processing of data are not preserved.

[40] https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_en.pdf pages 23-24.

[41] Bernh Larsen Holding AS and others v Norway (Application No 24117/08) (Judgement 2013), paragraph. 159.

3 Overview of Data protection definitions

The data protection terminology is important for the correct application of the data protection law especially in sensitive data processing. These concepts were first adopted by the Data Protection Directive and are essentially adopted also by the new General Data Protection Regulation. Nonetheless, in the new GDPR new elements are introduced

3.1 Personal Data

EU law and Council of Europe law define personal data as information relating to an identified or identifiable natural person (the data subject), which means information about a person whose identity is either manifestly clear or can at least be established by obtaining additional information[42] The definition of personal data is almost the same in Article 4.1 of the GPDR.

Identified person: Identification involve details which define a person in a way that he or she is distinguishable from other persons and recognizable as an individual such as an Identification Card Number or data containing name and surname combined with the birth date or home address.

Identifiable person: A person is identifiable when a piece of information includes elements of identification through which a person can be identified either directly or indirectly. Specifically, it refers to information that although do not associate with a name directly, can, with further research, lead to the identification of a person. Such details are for example an Internet Protocol (IP) address, location data (for example the location data function on a mobile phone)[43] or data held by a hospital or doctor, which could be a sign that uniquely identifies a person. Whether specific information is or not personal data requires de facto analysis of the particular case.

[42] Article 2(a) of the Data Protection Directive and Article 2(a) of the Convention 108.

[43] Note that in some cases, there is a specific sectoral legislation regulating for instance the use of location data or the use of cookies the ePrivacy Directive (Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 (OJ L 201, 31.7.2002, p. 37) and Regulation (EC) No 2006/2004) of the European Parliament and of the Council of 27 October 2004 (OJ L 364, 9.12.2004, p. 1).

Recital 26[44] of the Data Protection Directive set the benchmark for identifiability. That is whether it is possible that reasonable means for identification will be accessible and managed by all the foreseeable users of the information. The GDPR has the same approach as the DPD but embraces a more *precise definition* of "identifiable person" in Article 4(1).

The applicability of Data Protection law is not affected by the form in which personal data are stored or used. Personal data may be included in written on paper and electronically held information, in biometric data (e.g. fingerprints) and even cell samples of human tissue which hold and record DNA of an individual person.

Processing of Personal Data

Processing covers a wide range of operations performed on personal data. Forms of personal data processing include collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, alignment or combination, restriction, erasure or destruction of personal data. The way of process can be either with automated or by manual means. Actions where the data leave the responsibility of a Controller and are transferred to the responsibility of another Controller are also processing of personal data. Article 4(2) and (6) of the GDPR provides for the official definition of "processing". The term "processing" is presented likewise in Article 2 (b) of the DPD and in article 2 (c) of the Convention 108. Under EU law "processing" is besides the manual processing of structured filing systems.[45].

In the case of *Bodil Lindqvist, for example,* The Court has held that "*the act of referring, on an internet page, to various persons and identifying them by name or by other means (giving their telephone number or information about their working*

[44] (26) *"Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the Controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible*;" Data Protection Directive EU Directive 95/46/EC

[45] In Convention 108 processing of data files which are not processed automatically also must be protected Article 3.2 (c) of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*

conditions and hobbies) constitutes "the processing of personal data wholly or partly by automatic means". Moreover, reference to the state of health of an individual amounts to processing of data concerning health within the meaning of the 1995 directive"[46].

Other examples of processing can be staff management and payroll administration; access to/consultation of a contacts database containing personal data; sending promotional emails; shredding documents containing personal data;[47]

Data subject

A data subject is any person whose personal data is being collected, held or processed. Personal data can refer to anything from a person name, home address or ip address. As a result, anyone can become a data subject. As mentioned before[48] EU data protection law does not, in principle, protect the data of legal persons. Similarly, Convention 108 refers primarily to naturals persons. Nonetheless, the domestic regulators can extend data protection to legal persons according to article 3.2 (b) of the Convention 108.

Data Controller and Data Processor

In Chapter 1, Article 4 of the GDPR the two notions are defined as below:

"Controller" is "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*."

"Processor" refers to "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller*."

The respective article in Data Protection Directive about the data Controller and the data Processor is Article 2(e) and in Convention 108 Article 2(d). The concepts of data Controller and data Processor remain the same under the GDPR as they were under DPD. However, GDPR introduces a new concept of "joint Controllers" in Article

[46] Judgment of the Court in Case C-101/01, Bodil Lindqvist

[47] https://ec.europa.eu/info/law/law-topic/data-protection/reform/what constitutes-data-processing_en

[48] See chapter 2

26 when two or more Controllers together decide the purposes and means of the processing of data. Moreover, GDPR regulates differently the Controller-Processor-data subject relationship.

- Controllers under GDPR have a high duty to select the Processors with diligence by implementing "*appropriate technical and organizational measures*" and by using "*only Processors providing sufficient guarantees*"[49]. There must be a binding contract between the Processor and the Controller under Article 28.3 which lists also specific elements to be included in these contracts, such as duration of the processing, nature and purpose of the processing, the type of data and categories of data subjects as well as the rights and the obligations of the Controller.
- Processors under GDPR have certain obligations and might be held responsible for not complying with them. Data subjects whose personal data rights have been infringed have the right to an effective judicial remedy against the data Controller or against the data Processor and claim compensation from the responsible one.
- Processors are under an obligation to maintain a record of all categories of processing activities. This must include details of the Controllers and any other Processors and of any relevant Data Protection Officers (DPOs), the categories of processing carried out, details of any transfers to third countries and a general description of technical and organisational security measures. These records must be provided to the supervisory authority on request. If the Processor has fewer than 250 employees it is not mandatory except where the processing poses a risk to the rights and freedoms of individuals, is not more than occasional and does not include sensitive personal data.

Data Controllers and data Processors have different tasks and responsibilities. Data Controller is responsible to decide the process of personal data of other persons and data Processor processes these data on behalf of the Controller. In order for the data processing to be lawful the data Controller must supervise and inspect the actions of the Controller. There is also the case where a Processor can become a Controller if he breaches the instructions of the Controller and starts using the data for his or her

[49] Article 28.1 of the GDPR

own purposes. Either Controllers or Processors can be public authorities, agencies, natural or legal persons.

Definition of Sensitive Data

Sensitive data are special categories of data which by their nature may impose a greater risk to the data subjects and need enhanced protection. In principle, the processing of sensitive data is prohibited and is permitted only in exceptional circumstances combined with strict safeguards and special conditions.

Article 6 of the Convention 108 defines sensitive data all personal data that reveal:

- Racial or ethnic origin
- Political opinions, religious or other beliefs
- Health or sexual life

The Data Protection Directive in Article 8 (1) repeats the categories mentioned in Convention 108 but also it adds “trade union membership”. The new GDPR in article (1) expands the categories of sensitive data list and include *genetic and biometric data*, which if processed will lead to the unique identification of a person.

Sensitive vs. non sensitive data

GDPR and DPD present similar rules in that in principle they both prohibit the processing of special categories of personal data. The DPD, in Article 8 defines that all Member States shall prohibit the processing of sensitive data, with the exemptions laid down in paragraph 2, such explicit consent, vital interests etc.

The GDPR, in Article 9.2, generally replicate the provisions of the DPD in this matter. Explicit consent is still a prerequisite for processing personal sensitive data, but with additional conditions (see chapter 4 and 6 for analytical presentation of consent). Furthermore, in some issues grounds for the processing of sensitive data have been extended in GDPR.

Material Scope of Data Protection Law

Under DPD, Article 3, the material scope of data protection is very broad. It applies in both automated and manual processing with two exceptions: a) if the processing is in the course of purely personal or household activities b) if the processing falls outside the scope of European Union Law for example issues concerning national security of a Member State.

GDPR applies to "*the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system*" as stated in Article 2.This Regulation does not apply to the processing of personal data:

(a) In the course of an activity which falls outside the scope of Union Law;

(b) By the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TFEU, for example policies in border control, asylum and immigration procedures etc[50];

(c) By a natural person in the course of a purely personal or household activity;

(d) By competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

The activities that fall outside of the scope of the Union Law are mentioned both in DPD and GDPR. This exemption is not strict and gives the Member States the right to legislate the appropriate measures and laws

The exception of personal or household activity raised the issue of the difficulty to distinguish which processing is purely personal or not. The distinction becomes difficult because the rise of social networks gave individuals the power to publish their own personal data but unavoidably in many cases publishing the personal data of others. Before the new GDPR Article 29 Working party provided some guidelines in order to easier distinguish if the processing regards personal or household activities[51].

[50] https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:12012M/TXT

[51] Annex 2: Proposals for Amendments regarding exemption for personal or household activities online https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf

Territorial Scope of Data Protection

The territorial scope of Data Protection is very important in order to delineate the extent to which the GPDR is applicable to the processing of personal data in the EU/EEA region and outside of it when there is a connection with the EU/EEA territory especially in medical data field and clinical research where organisations from EU and other non EU countries may be involved.

The European Economic Area (EEA) consists of 28 Member States, with Norway, Iceland and Liechtenstein as members of EFTA[52].

The territorial scope of GPDR is set out in Article 3 and defines broadly the term. Businesses that are established in a Member State must comply with the new Regulation, exactly as they pertain to DPD. But the new Regulation, unlike DPD, introduces wider conditions for applicability of the GDPR. The key differences are the following:

- When Processor or Controller is established in the Union, the GDPR, according to article 3, will apply to the processing of personal data in the "*context of the activities*" of a Controller or Processor in the EU, regardless the place of the processing. Under DPD the criteria for determining the applicable law was the location of the "*establishment*" of the Controller and the location of the means or equipment used for the processing of data. DPD did not refer at all to the location of the Processor in Article 4.
- When the Processor is not established in the EU the GDPR requires compliance with the EU Data Protection Law in case the business processes personal data about EU data subjects in connection with the "offering of goods or services" (payment is not required); or "monitoring" their behaviour within the EU. It must be apparent that the organisation "envisages" that activities will be directed to EU data subjects. Moreover, GDPR will apply when Member State law is applicable to that place by the virtue of public international law. DPD on the other hand although it mentions that national law should be applicable to that place by virtue of public international law it only refers to

[52] The European Free Trade Association (EFTA) is the intergovernmental organisation of Iceland, Liechtenstein, Norway and Switzerland. EFTA was founded by the Stockholm Convention in 1960. Relations with the EEC, later the European Community (EC) and the European Union (EU), have been at the core of EFTA activities.

cases when the equipment used for processing was situated on Member state territory unless it was used only for purpose of transit.

- Article 27 of the GDPR imposes the obligation to designate, in writing, a representative in the EU in the case a company is established outside EU. This obligation does not apply to public authorities or bodies, when the processing is occasional, does not include processing operations with special categories of data on a large scale (Article 9(1)) or concerns personal data relating to criminal convictions and offences (Article 10), if these types of processing are unlikely to result in a risk to the rights and freedoms of natural persons. Article 4.2 of the Directive, provides for any data Controller not established in the EU is required to designate a representative in each EU member state in which it meets the 4.1(c) requirements

- The term "establishment" has been interpreted by the CJEU as a ""*broad" and "flexible" phrase that should not hinge on legal form. An organisation may be "established" where it exercises "any real and effective activity – even a minimal one" – through "stable arrangements" in the EU. The presence of a single representative may be sufficient*"[53]. In the same case the Court has stated that in the "*context of activities*" international business have to demonstrate that there is no commercial connection between a local branch or subsidiary and a non EU company Controller in order for the DPD not to apply to data processing by a company Controller established outside EU[54]. In the Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González the Court gave a broader definition to the term "*context of activities*". As stated by the Court decision "*processing of personal data is carried out in the context of the activities of an establishment of the Controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space*

[53] Judgment of the Court (Third Chamber) of 1 October 2015, — Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság, (Case C-230/14)

[54] See also: Article 29 Working Party Opinion 8/2010, "Opinion 8/2010 on applicable law" 16 December 2010

offered by that engine and which orientates its activity towards the inhabitants of that Member State"[55].

4 Key Principles and Rules of the European Data Protection Law

4.1 Structural Safeguards

Convention 108 provides a legal framework with effective safeguards and basic principles for data protection. Specifically, personal data shall be "*obtained and processed fairly and lawfully*", "*stored for specified and legitimate purposes*", preserved in a form that "permits *identification of the data subjects for no longer than is required*", the data should be "*adequate, relevant and not excessive in relation to the purposes for which they are stored*" and "*accurate and kept up to date*"[56].

In Article 6 of the Convention 108 stricter requirements are laid out regarding *special categories of data*: "*Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions*".

Additional safeguards of the Convention 108 are "*data security appropriate security measures*"[57]. Article 8 sets safeguards for the data subject such as access to his or her personal data, "*rectification or erasure of such data if these have been processed contrary to the provisions of domestic law*", remedy if the requests of the data subjects are not complied with.

The Data Protection Directive enshrines the same principles as Convention 108, however with more specifications and with the addition of further requirements and

[55] See also: CNIL's Google Decision Délibération No 2013-420 du 3 janvier 2014 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société X

[56] Article 5 – Quality of data, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, (1981)

[57] Article 7 Data security, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data(1981)

conditions[58]. The GDPR sets the basic principles in Article 5. Restrictions or exemptions from the key principles may be provided for at a national level only if three conditions are fulfilled: they are provided for by law, pursue a legitimate aim and are necessary in a democratic society.

Lawful processing

Article 6 of the Data Protection Directive and article 5 of the new GDPR lay out the first principle of *lawful processing*. ECtHR jurisprudence has interpreted the meaning of lawful processing in connection with justified interference under Article 8.2 ECHR and CJEU jurisprudence defined the conditions for lawful limitations under Article 52 of EU Charter[59].

GDPR introduces strict conditions for lawful processing in Articles 6-10 especially in special categories of data, called *sensitive data*.

The processing of Sensitive Personal Data is only permitted under certain conditions[60]:

Sensitive Data Processing

Lawful Basis	Data Protection Directive	GDPR	Analysis
Explicit consent	According to Article 8.2. (a) "*The data subject has given explicit consent*".	According to Article 9.2. (a) "*The data subject has given explicit consent*".	Explicit consent means that the data subject must take some positive actions to signify consent and to be free not to consent. This can be oral or writing.
Vital Interests of the Data Subject	"*The processing is necessary to protect vital interests of the data subject (or another person) where the data subject is incapable of giving consent*" under Article 8.2.(c).	"*The processing is necessary to protect vital interests of the data subject (or another person) here the data subject is incapable of giving consent*» under Article 9.2. (c).	This constitutes a lawful base if the data subject is physically or legally incapable of giving consent.
Legitimate Interests of others	Article 8.2	Article 9.2 (b)	Recitals 47-50 of GDPR give the

[58] Article 6, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[59] See Chapter 3 for detailed presentation of lawful limitations and justified interference.

[60] Sensitive Data processing will be examined in detail in the following chapters about *Health Data Processing* and *Scientific Research*.

	(b)"*The processing is necessary in the context of employment law*", (d) "*The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, or persons with whom it has regular contact in connection with its purposes"*. (e) "The processing relates to personal data which have been manifestly made public by the data subject" and "*The processing is necessary for the establishment, exercise or defense of legal claims*".	"*The processing is necessary in the context of employment law, or laws relating to social security and social protection*". (d) "*The processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes*". (e) "*The processing relates to personal data which have been manifestly made public by the data subject*". (f) "*The processing is necessary for the establishment, exercise or defense of legal claims, or for courts acting in their judicial capacity*".	definition of what may be considered "legitimate interest». Legitimate interests of others cannot longer be a basis for public authorities when they process personal data in the exercise of their functions.
Public Interest		According to Article 9.2.(g) "*The processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is, inter alia, proportionate to the aim pursued and protects the rights of data subjects*".	Member States can introduce further purposes for processing sensitive data.
Medical Diagnosis and Treatment	Article 8.3 *"The processing is required for the purpose of medical treatment undertaken by health professionals"*.	Article 9.2 (h), 9.3 "*The processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the management of health or social care systems and services*".	GPDR added in the medical diagnosis and treatment basis the case of employee's health and the management of health or social care systems and services.
Historical, statistical or scientific purposes	N/A	Article 9.2(j) "*The processing is necessary for archiving purposes in the public interest,*	These purposes "shall be subject to appropriate safeguards." Data

		for historical, scientific, research or statistical purposes, subject to appropriate safeguards".	minimization, anonymisation and data security are mentioned as possible safeguards[61].
Exceptions under national law	Member States can for reasons of public interest, lay down additional exemptions.	Article 9.4 "*Member States may maintain or introduce further conditions, including limitations with regard to genetic data, biometric data or health data*".	GDPR introduces a research exemption to the general prohibition of sensitive personal data processing.
Public Health	N/A	Article 9.2(i) "*The processing is necessary for reasons of public interest in the area of public health"*	*Reasons of public interest* may be protecting against serious cross border threats to health or ensuring high standards of healthcare and of medicinal products or medical devices

Purpose specification and limitation

Personal data collected for one purpose should not be used for a new, incompatible, purpose. In Data Protection Directive article 6.1 (b) stipulates that personal data shall only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes is permitted, provided that Member States provide appropriate safeguards[62]. GDPR repeats that personal data must be processed according to the purposes that explicitly enumerates. Transfer of data to third parties is a new purpose which needs also an additional legal basis.

Data "Minimization", Accuracy and Storage Limitation

The Controller must implement in all processing operations the data quality principles.

[61] Article 29 Working Party Guidelines on consent under Regulation 2016/679, Adopted on 28 November 2017 As last Revised and Adopted on 10 April 2018,

[62] Article 89 Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

- Data minimization: Personal Data in order to be processed must be adequate, relevant and limited to the necessary in relation to the purpose for which they are collected. In comparison with Article 6.1 (c) of DPD[63], GDPR introduces a more restrictive obligation to ensure that personal data are «….*limited to what is necessary in relation to the purposes for which those data are processed.*" in Article 5.1(c).
- Accuracy: Controllers have the obligation to ensure that personal data are accurate. The accuracy of the data must be examined in the context of the purpose of data processing.
- Storage Limitation: The principle is unchanged, in relation with Convention 108 and DPD Article 6.1(e) and the data must be erased when the purposes for which they were collected are served, but GDPR in Article 5.1(e) defines that if the data were collected solely for public interest, or scientific, historical, or statistical purposes they can be stored for longer periods.

Fair and Transparent Processing

Fair and *Transparency processing* means that the controller is obligated to explain the process operation to the data subject in an easy and understandable way, ensure that the data subject can access his or her data, understand fully the purpose their data will be used for and who is the Controller. Unless specifically permitted by law the processing of personal data must not be performed in secret. Article 6.1.(a) of the Data Protection Directive states that "*Personal data must be processed fairly and lawfully*". Article 5.1. (a) of the GDPR added "*in a transparent manner in relation to the data subject*" requiring that Controllers take additional care when designing and implementing data processing activities.

Accountability

The General Data Protection Regulation (GDPR) integrates *accountability* as a principle which guarantees the enforcement of the Data Protection Principles. Under the GDPR, the Controller is obliged to demonstrate that its processing activities are

[63] "*Personal data must be adequate, relevant and not excessive in relation to the purposes for which those data are collected and/or further processed*".

compliant with the Data Protection Principles which was not an obligation under the previous Directive 95/46/EC. GDPR's new accountability obligations require the adoption of new technical and organizational measures to demonstrate compliance. These obligations include privacy by design, security breach notifications to Data Protection Authorities, appointment of a representative Controller or Processor established outside the EU and the conduct of Privacy Impact Assessment when the processing involves high risk data[64]. In Article 31 and 32 GDPR introduces a personal data breach notification regime. In the case of personal data breach the Controller must without any delay, not later than 72 hours after being aware of it, notify the Supervisory Authority competent in accordance with Article 51.

Integrity and Confidentiality

According to Articles 5.1.(f), 24.1, 25.1, 28, 39 and 32 of the GDPR personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

Key Rules on Security of processing and Transparency

According to Article 32 the Controller and the Processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

Article 12 of the Regulation outlines the rules on *Transparency*. The WP29 guidance also notes that individuals should be able to determine the scope and consequences of data processing. Controllers must be clear about how the processing will affect the data subject[65].

[64] ARTICLE 29 DATA PROTECTION WORKING PARTY, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", As last Revised and Adopted on 4 October 2017

[65] ARTICLE 29 DATA PROTECTION WORKING PARTY, "Guidelines on transparency under Regulation 2016/679", As last Revised and Adopted on 11 April 2018

5 Data Subject Rights

The new GDPR (Chapter 3, articles 12-23) empowered the rights of the data subjects under DPD[66] and created new ones.

Right to object

The data subject must be informed on his or hers right to object (Article 21.5) and the objection right can be expressed verbally or in writing. The right to object is a general right which can be limited only in certain cases such as specific legal obligations. Secondly, the right to object includes the data subject's right to be informed, free of charge, and can be raised by the data subject without any justification. GDPR provides for that the data subject shall have the right to object at any time but in the following circumstances the right to object is not absolute:

a) Processing is based on legitimate interest according to Article 6.e or on the necessity to perform a public interest task (Article 6.f) including profiling. The principle of proportionality must apply in order for the Controller to continue processing (Article 21.1)

b) Processing is made for scientific/historical research/statistical purposes but not when the processing is performed for reasons of public interest (Article 21.6).

The GDPR, unlike DPD which required the data subject to prove that the objection was justified[67], requires the Controller to demonstrate that he either has compelling grounds for continuing the processing, or that the processing is necessary in connection with his legal rights. Otherwise, he must cease that processing activity. GDPR Article 21.2-3 is similar to Article 14(b) of the Directive but it adds "*profiling*". "*Profiling*" refers to a set of data characterizing a category of individuals that is intended to be applied to an individual. According to the definition laid out by the

[66] A similar right is maintained in GDPR (Recitals 50, 59, 69-70, 73; Article 21) which aims at the balance between the right of data subject in protection and the legitimate right of those who process the data.
[67] Recital 30, 45; Article 14(a), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Committee of Ministers "*Profiling" means an automatic data processing technique that consists of applying a "profile" to an individual, particularly in order to take decisions concerning her or him or for analyzing or predicting her or his personal preferences, behaviours and attitudes*[68]. Moreover, automated processing in Recital 71, 75 and Article 22 of the GDPR requires explicitly consent of the data subject and appropriate safeguards. Automatic processing is also permitted if:

- *it is necessary for entering into or performing a contract with the data subject provided that appropriate safeguards are in place;*
- *it is authorised by law;*

According to Recital 59 and Article 12.3-4 of GDPR the Controller must provide any requested information in relation to any of the rights of data subjects within a month of the request. Under the previous Directive there were no specified time limits.

In case of a breach of their rights data subjects have remedies available in national level in different ways:

- the right to lodge a complaint with supervisory (Article 77) ;
- the right to an effective judicial remedy where a competent supervisory authority fails to deal properly with a complaint (Article 78) ;
- the right to an effective judicial remedy against a Controller or Processor(Article 79);
- the right to compensation from a Controller or Processor for material or immaterial damage resulting from infringement of the Regulation (Article 82).

Article 83 of the Regulation establishes the general conditions for imposing administrative fines. The GDPR sets out significant changes in maximum fines of the greater of €20 million or four percent of an undertaking's worldwide turnover[69]. There

[68] Recommendation CM/Rec(2010) of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling *Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies* The Committee of Ministers,

[69] The CJEU has held that the term *undertaking* "encompasses every entity engaged in an economic activity, regardless of the legal status of the entity and the way in which it is financed", Judgment of the Court of 17 February 1993 - Christian Poucet v Assurances Générales de France and Caisse Mutuelle Régionale du Languedoc-Roussillon**,** Joined cases C-159/91 and C-160/91

are, furthermore, international remedies available. The data subject may bring violations before the ECtHR and the CJEU but only to a very limited extent[70].

Right to access

Article 8.2 of the Charter of Fundamental Rights and Article 12 of the Data Protection Directive contain the aspects of the data subject's right of access. The ECtHR has held that the right to access information about one's personal data derives from the need to respect private life[71] .The right to access is the right of any individual to obtain information from the Controller about the data that is being processed, the purposes for which they are used for and any automated decision process concerning him or her. GDPR enriches the mandatory categories of information which must be supplied when the data subject requests access in Article 15. In comparison to Data Protection Directive, the Regulation adds information about the period for which the data will be stored, the existence of rights to erasure, rectification and objection of the individual, the right to complain to the Data Protection Authority, where the data were not collected from the data subject information as to the source of the data and the existence of automated processing that has a significant effect on data subjects.

Nonetheless, there are some restrictions to the right to access when personal data are stored by public authorities. In the case Leander v. Sweden the ECtHR concluded that the right to access might be limited in certain circumstances[72] a)overriding legal interests of others b) data processed by scientific purposes and that the right to access may not be restricted by undue time limits[73].

Right to rectification, erasure and data portability

Right to rectification provides the data subject the power to ask for modifications to his or her personal data in case the data subject regards that this personal data is not up to date or accurate (Recitals 39, 59, 65, 73 and Article 5.1(d), 16

[70] Article 263.4 and Article 267 of the TFEU
[71] Case of Gaskin v. the United Kingdom, *(Application no. 10454/83)*, **(**Judgement 1989), paragraph 39
[72] Case of Leander v. Sweden, (Application no. 9248/81), Judgment 2 March 1987,
[73] College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer, Case C-553/07, Judgment of the Court (Third Chamber) of 7 May 2009, paragraph 59

of GDPR). The Directive (Article 6.1d), 12(b)) and the GDPR address this right in the same way.

Right to erasure known as the "*right to be forgotten*" is the right of a person to request for personal data to be erased once the data is no longer necessary. When the consent is withdrawn or when certain data are not anymore necessary to fulfill the purpose of the processing the legitimate basis ceases to exist. This is not an absolute right, and has to be examined de facto. According to the principle of accountability the Controller must demonstrate that there is a legal basis to its data processing otherwise the processing must stop.

Right to data portability means that the data subject can request his or her personal data to be transferred in another Controller. It is a new possibility introduced by the Regulation in Article 20. GDPR does not require specific file formats, but WP29 notes that "*a format that can only be read subject to costly licensing constraints would be considered inadequate*"[74].

6 Privacy rights and Health Data

Personal health data including information on drug usage, prescriptions, and other medical records and information account to some of the most sensitive data. Today new technologies facilitate the digitalization of medical information in the form mostly of Electronic Health Records. While, digitalization of Health Records is important for improving and revolutionizing healthcare services the use of Electronic Health Records carries enormous risks for privacy and security. Many questions arise such as who can access the health records of a person; what kind of information these records will contain; can anyone use a person's personal data without informing him or her and how important is consent in medical data processing. In clinical research the new Regulation will bring the need for operational changes and appropriate controls in the research field. Medical data is subject to stricter data-processing regime than non-sensitive data.

[74] ARTICLE 29 Data Protection Working Party, "Guidelines on the right to data portability" Adopted on 13 December 2016.

The GDPR continues to treat health data as sensitive personal data like the Data Protection Directive used to. The GDPR, in particular, adds genetic data and biometric data as sensitive personal data and allows Member States to bring in additional conditions in the processing of biometric, genetic, and health data.

6.1 Regulatory framework

Medical Data as Recommendation No.R (97)5 on the Protection of Medical Data states in Article 1 are "*all personal data concerning the health of an individual. It refers also to data which have a clear and close link with health as well as to genetic data*"[75]. They refer not only to data held by a doctor about patients but to any person likely to keep medical data. Data concerning the state of health of the data subject are qualified as sensitive data both under EU and CoE law, specifically in Article 8.1 of the Data Protection Directive, Article 9 of GDPR and Article 6 of Convention 108. GDPR moreover, introduces genetic and biometric data as sensitive personal data. All data contained in medical documentation, in electronic health records and systems should be considered to be sensitive data[76].

Medical data in an electronic health record or recorded on paper may be:

- General numerical information.
- Diagnostic-related information, laboratory test results, genetic tests, imagery.
- Treatment information. Prescribed drugs, dosage, effects, and surgeries.
- Medical correspondence with the doctor.
- Administrative data, such as hospital social security patient information.
- Claims data, in case of private insurance claims.
- Patient/disease registries in hospitals or clinics.

There are general EU regulations applicable to privacy and data protection and sector specific instruments that compound the regulatory framework for medical data processing. It is important that any processing concerning medical data must follow and comply with the general rules and principles of personal data processing[77].

---

[75] Council of Europe, Committee of Ministers, Recommendation No. R (97) 5 on the Protection of Medical Data (Feb. 13, 1997).

[76] ARTICLE 29 Data Protection Working Party, "*Working Document on the processing of personal data relating to health in electronic health records (EHR)*"Adopted on 15 February 2007.

[77] For detailed presentation see Chapter 4.

The general health data protection framework encompasses Article 8 of the ECHR, Articles 7 and 8 of the EU Charter along with Article 6 of Convention 108, the Data Protection Directive and the new GDPR. Both the DPD and the GDPR protect and distinct certain categories of personal data and state that these categories of data require extra protection and can be processed only if special conditions apply and only for specific purposes[78]. The case law of ECtHR, in addition, has in many cases established that the collection and storage of medical data or any unauthorized access to these data is an infringement of patient's right to private life according to Article 8 of ECHR[79]. Data subjects, as mentioned before, have also the right to bring their case before CJEU under certain circumstances that Article 263.4 and Article 267 of the TFEU provide for.

Furthermore, there are health sector specific instruments which consist of detailed principles and guidelines for the protection of privacy and data protection. They are significant in order to interpret CoE and EU law in the health field:

- Council of Europe has published *Recommendation 97 on Medical Data Protection*[80] and *Medical Data Protection Explanatory Memorandum*[81]. Both apply principles of Convention 108 to medical data processing in detail.
- Instruments of European Union are the *Article 29 Working Party EHR Report*[82] and the *European Commission's eHealth Action Plan 2012-2020*[83]*. Article 29 Working Party EHR Report* notably states that "*considering the impact of EHR systems and the special need for transparency of such systems the safeguards should preferably be laid down in a special comprehensive legal framework*" and provides detailed presentation

[78] Ibid.

[79] For example see Case Avilkina and others v. Russia, Judgment of 6 June 2013, (Application No. 1585/09).and Case I. v. FINLAND, Judgment of 3 April 2007, (Application No. 20511/03)

[80]Council of Europe, Committee of Ministers, "*Recommendation No. R (97) 5 on the Protection of Medical Data"* (1997).

[81]"*Explanatory Memorandum Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes"*, Adopted by the Committee of Ministers on 30 September 1997 at the 602nd meeting of the Ministers' Deputies

[82] ARTICLE 29 Data Protection Working Party, "*Working Document on the processing of personal data relating to health in electronic health records (EHR)*", Adopted on 15 February 2007

[83] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "*eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century",* Brussels, 6.12.2012

of derogations from general prohibition of processing sensitive data. *EHR Report*[84] and the *European Commission's eHealth Action Plan 2012-2020* focuses on the patients and healthcare employee's empowerment, on research innovation and future technologies in the medical sector. The Action Plan also addresses issues around "mobile health" (mHealth) and health & wellbeing applications. After the Action Plan the Commission also published the *Green Paper*[85] and the *STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps*[86] which repeat that the "*processing of personal data concerning health is in principle prohibited as these data are considered sensitive*".

6.2 Processing Health Data

Under Data Protection Directive in Article 8.1 and the new Regulation in Article 9.1 processing of personal data concerning health is prohibited. Article 6 of the Convention 108 also prohibits processing of sensitive data. This is a general prohibition and both DPD and GDPR set similar grounds for processing medical data, although the new Regulation widens the grounds for the processing in the area of health management[87]. Member States may limit or expand the conditions regarding health, biometric and genetic data if they consider it appropriate.

The importance of these data, of course, in order to medically treat patients, requires exemptions from the general prohibitions of processing medical data. These derogations are laid out in Article 8.2, 8.3 and 8.4 in Data Protection Directive and in Article 9.2 and Recitals 51-54 of the Regulation. It is worth noting that all these derogations are limited and exhaustive.

The exemptions are examined separately.

---

[84] ARTICLE 29 Data Protection Working Party, "*Working Document on the processing of personal data relating to health in electronic health records (EHR)*", Adopted on 15 February 2007

[85] European Commission, "*GREEN PAPER on mobile Health ("mHealth")*", Brussels, 10.4.2014

[86] *" COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps Accompanying the document GREEN PAPER on mobile Health ("mHealth*")", Brussels, 10.4.2014

[87] Article 9.2.(h) of GDPR

Explicit Consent

Data Protection Directive in Article 8.2 stipulates that "*Paragraph 1 shall not apply where the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent*". GDPR in Article 9.2(a) also requires explicit consent of the data subject with the exception when the laws of EU or a Member State define differently.

In Recital 32, Article 4.11 and 6.1(a) of GDPR, "consent" means any "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*". "*Freely given*" the consent must be a genuine choice of the data subject and not a result of intimidation, misleading, deception, coercion or fear about negatively impacts by withholding consent[88].

"*Unambiguous*" means that the consent must be collected in a manner that undoubted indicates the data subject's intentions in providing their agreement to their personal data being processed.

"*Statement or clear affirmative action*" is the case when a person takes deliberate and specific action to opt in or agree to the processing. This includes for example signing a consent statement, oral confirmation, a binary choice presented with equal prominence, but it does not include silence inactivity, default settings or pre-ticked boxes[89]. The consent must not contain ambiguity but a positive action. Valid consent must be both unambiguous and affirmative.

"*Specific*" consent is another element of valid consent and is directly related to personal data processing purposes. Specific consent is besides strongly linked with the element of informed consent. GDPR in Recital 42 states that: "*for consent to be informed, the data subject should be aware at least of the identity of the Controller and the purposes of the processing for which the personal data are intended*"**.** For the

[88] Article 29 Working Party "*Article 29 Working Party Guidelines on consent under Regulation 2016/679*" Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2018

[89] Information Commissioner's Office Consultation: "GDPR consent guidance", draft, 31 March 2017, www.ico.org.uk

consent to be specific it must be in an easily accessible form. The Controller must clearly and precisely define the scope, the purposes and the consequences of the data processing[90].

"*Informed*" consent means the consent based upon an understanding and an evaluation of the true facts and repercussions of his actions. The right to be informed applies no matter whether consent is required or not. The Article 29 Working Party guidelines[91] on consent have defined the following information that must be demonstrated to obtain valid, informed consent, along with article 13 of the Regulation:

- Identity of the Controller.
- Purpose of each processing operation where consent is the legal ground.
- Data and type of data that will be collected and used through consent.
- Information about the right to withdraw consent.
- Information regarding the use of data for decisions which are solely based on automated processing, including profiling.
- The possible risks of data transfers to third countries
- The recipients of possible transfers of data.

The consent must also be "*explicit*" in the processing of sensitive data. Opt out choices do not satisfy the requirement of "*explicit*" consent. In GDPR, there are two types of consent "*unambiguous"* consent according to Article 4 and "*explicit*" consent according to Article 9.1. Under GDPR Article 9 "*explicit*" consent is required for the processing of certain "special" types of personal data. But is there a difference between "*unambiguous"* consent and "*explicit*" consent? Not all consent that is unambiguous is simultaneously explicit. "*Explicit*» consent is an "*explicit statement"* regarding the specific personal data to be collected and an explicit action by the subject agreeing with this *statement*. In other words the data subject must opt-in in sensitive data. "*Unambiguous"* consent requires the "*clear affirmative action*" for example "*by filling in an electronic form, by sending an email, by uploading a scanned*

[90] A general agreement of the data subject for example for collection and processing of his medical data of the past and of the future from doctors involves in his treatment is not valid consent.
[91] ARTICLE 29 Data Protection Working Party "Article 29 Working Party Guidelines on consent under Regulation 2016/679" Adopted on 10 April 2018

document carrying the signature of the data subject, or by using an electronic signature"[92].

There are many judgments of the ECtHR concerning the matter of lack of consent and disclosure of medical data. In *L.L. v. France* case the Court held that the use of the applicant's, without his consent, by the judge of a confidential medical document, namely the correspondence between the applicant's doctor and a specialist was a violation of his private life under Article 8 of the European Convention on Human Rights. The medical document had been used by the judge only on a secondary basis and the French Court had not justified the interference in view of the fundamental importance of protecting personal data[93]. Another important case is *Y.Y. v. Russia*[94]. The applicant complained that the St Petersburg Committee for Healthcare had collected and examined her medical records and those of her children and forwarded its report containing the results of its examination, to the Ministry of Healthcare without her consent. The Court found a violation of Article 8 because the actions in dispute did not constitute a foreseeable application of the relevant Russian law.

The individual can withdraw consent at any time and must be informed of that right prior to giving consent.

For children below the age of 16, parental consent is necessary for the processing of data to be lawful. However, Member States may decide to lower that age, but not below 13 according to Article 8 of the GDPR.

To carry data Controller's obligations in employment law

Article 8.2 (c) of the DPD provided for that in case of sensitive data an exception exists when "*processing is necessary for the purposes of carrying out the obligations and specific rights of the Controller in the field of employment law insofar as it is authorized by national law providing for adequate safeguards*». Article 9.2 of the GDPR allows sensitive data processing when it is necessary for the fulfillment of obligation under employment, social security, social protection law or collective

[92] Ibid.
[93] L.L. v. France - *Application No 7508/02 Judgment 10.10.2006 [Section II]
[94] Y.Y. v. Russia, Judgment of 23 February 2016, *Application no. 40378/06)

agreement. The Regulation has expanded the scope of this derogation as compared to the DPD by requiring compliance with collective agreements and obligations under social security and social law. Furthermore, Recital 52 of the GDPR clarifies that "*Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health*. *Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*".

Legitimate activities of non profit

Article 8.2 (d) of the Data Protection Directive provided for that processing is allowed when "*is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects".* The new Regulation does not present changes in Article 9.2 (d) about the sensitive medical data processing in regard with the nonprofit bodies.

Processing of data related to criminal offences and civil claims

Article 10 of the GDPR provides for that "*Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1)*

shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority". The Regulation regards criminal data as sensitive data as the Directive did in Article 8.1.

Vital interests of the subject

This is an important derogation in the scope of medical data. Article 9.2(c) of the GDPR repeats the wording of the Data Protection Directive in Article 8.2 (c): "*processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent*". Recital 46 provides further assistance on the matter: "*The processing of personal data should also be regarded as lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis…*" The vital interests of the data subject are not cited in Article 8 of the ECHR. Nonetheless, the vital interests of the data subject are implied in the notion of "*legitimate basis*" of Article 5.2 of Modernized Convention 108 under CoE law[95]. The processing of sensitive personal data can be justified if it is necessary to protect the vital interests, life mainly, of the subject or of another person where the data subject is physically or legally incapable of providing consent. The processing must relate to essential individual interests of the data subject or another person and it must be crucial for a life-saving treatment in a situation where the data subject is not able to express his intentions and his wills. Nonetheless, if information is available that the data subject wouldn't have given his consent to process, no matter the important interests, this provision cannot be a lawful basis. That is why this exception must apply only to a small number of medical cases and could not justify processing of personal

[95]"Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (2018) Modernized Convention 108, paragraph 46.

medical data for purposes other than treatment of the data subject in a life threatening situation. Medical care that is planned in advance does not fall in this derogation. However, a processing may be based on the grounds of both public interest and the vital interests of the data subject or that of another person for example where there is a humanitarian emergency.

Data is public

According to Article 8.2 (e) of the DPD the processing is allowed" *where processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims*". GDPR has similar provisions in Article 9.2 (e) and (f). There is no adequate definition of the concept "*manifestly made public*" under GDPR; however, this exemption is lawful where it is unambiguous that the data subject has himself published his personal data in the public realm, for example, on his own social media account. In cases such as the publishing of personal data in a biography, in the press or on a public personal blog or website the intention is apparent[96]. The publication must result from a free decision of the data subject[97] On the other hand, there are cases where is difficult to understand or interpret the intentions of the data subject. For example, registering for a social network might include the acceptance of certain data protection rules which are updated and altered constantly. These rules often are long, detailed and dense. Most of the data subjects will not read them thoroughly before agreeing. In that way they give access to their personal data but without ever "manifestly make them public". Consequently, it is important to carefully use this exception as a lawful base and examine each case separately.

Reasons of public interest in the area of public health

The Data Protection Directive (95/46/ EC) allowed, except from the EU or Member State law, a data protection authority to lay down exceptions for reasons of

[96] ARTICLE 29 DATA PROTECTION WORKING PARTY ,17/EN WP 258 "*Opinion on some key issues of the Law Enforcement Directive (EU 2016/680*") Adopted on 29 November 2017

[97] Paul Voigt, Axel von dem Bussche, 2017," The EU General Data Protection Regulation (GDPR) A Practical Guide", Springer International Publishing AG, Switzerland

substantial public interest[98]. Article 9.2 (j) of the Regulation, in a narrower exception and with the introduction of proportionality, specifies that the reasons of substantial public interest must be on the basis of EU or Member State law*, "which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and interests of individuals"*[99].

Anonymisation and Pseudonymisation in Health

According to the principle of *limited retention of data,* that is envisaged in Article 5 (e) of the Convention 108 and the Data Protection Directive Article 6. 1. (e), personal data must be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.*" The time limitation for storing personal data applies, however, only to data kept in a form which permits identification of data subjects[100]. In the event that the Controller wants to store these data for a longer period of time and since they no longer serve their initial purpose he has to proceed to anonymisation.

Anonymised data are the data which don't contain any identifying elements. As Recital 2 of the GDPR defines, no element must exist in the information, which could, by exercising reasonable effect, serve to re-identify the person concerned. The risk of re-identification can be assessed by taking into account "*the time, effort or resources needed in light of the nature of the data, the context of their use, the available re-identification technologies and related costs*"[101]. Moreover, the anonymised data are no longer considered personal and therefore the Regulation does not apply. However, this rule has a noteworthy exception: whenever the data subject, for the purpose of

[98] Article 8.4 "*Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority*".

[99] see also Recital 54 of the GDPR

[100] Handbook on European data protection law, European Union Agency for Fundamental Rights, 2014 Council of Europe.

[101] Council of Europe, Committee of Convention 108 (2017), Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 January 2017, para. 6.2.

exercising his rights gives further information to the Controller facilitating his or her identification, those previously anonymised data become personal data again[102].

Pseudonymisation of data is the method of replacing identifying characteristics of data with a value, in any form and the data subject cannot be directly identified. *Pseudonymisation* just offers a limited protection for the identity of data subjects in a number of cases because identification can be done using indirect means. The pseudonymised information still constitutes personal data and therefore remains in the scope of the Regulation. According to Article 25.1 of the GDPR there are various uses of pseudonymisation as an appropriate technical measure for enhancing data protection, and is specifically mentioned for the design and security of its data processing[103]. The Explanatory Report of Modernized Convention 108 in paragraph 18 provides for that "*the use of a pseudonym or of any digital identifier/ digital identity does not lead to anonymisation of the data as the data subject can still be identifiable or individualised*". Article 25 of the GDPR, which addresses data protection by design, explicitly refers to pseudonymisation as an example of an appropriate technical and organisational measure that Controllers should implement to accommodate the data protection principles and integrate the necessary safeguards. Moreover, Pseudonymisation is recommended by the Regulation in the following cases:

- When processing is incompatible with the purposes for which the personal data was initially collected and processed.
- In the case of organisations that use personal data for historical or scientific research or for statistical purposes
- As an example of a method which best implements "privacy by design and default"
- It fulfills the data security obligations of the Regulation, for example in personal data breaches and notification.

[102] General Data Protection Regulation, Article 11
[103] European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law, 2018, Luxembourg: Publications Office of the European Union, 2018

6.3 Medical Secrecy and health data

Article 8.3 of the Data Protection Directive provided for that "*Paragraph 1 shall not apply where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy*". This article introduces the terms "special purposes", "necessary" and "secrecy and confidentiality" for the protection of health data. "Special purposes" refers to the processing of sensitive data for the specific purposes of therapeutic, diagnostic, after care health services but also the related administrative procedures of providing the aforementioned health services. Further processing of these data for purposes of medical research for example, is not allowed under the DPD. Moreover, the processing must be "necessary" meaning that any processing of health data should be soundly justified. The third condition is that the processing of sensitive personal data by medical or other staff is subject to professional medical secrecy. Article 90.1 of the GDPR introduces a different approach in professional secrecy, by stating that it is in a Member State's discretion to adopt rules about secrecy and that the rules adopted by a Member State enacting "*an obligation of professional secrecy or other equivalent obligations of secrecy*" must be in the context of necessity and proportionality in order to harmonise the right of data protection and the duty of secrecy. According to Article 90.2 of the GDPR Member States were obliged to notify the Commission about "*the rules adopted pursuant to paragraph 1, by 25 May 2018 and, without delay, any subsequent amendment affecting them*". Non medical staff that also processes sensitive data has the same professional obligation to confidentiality and protection. Every professional engaged in processing of sensitive data is a Processor under Article 4 of GDPR and should comply with the requirements of the Regulation and carry out the processing stringently under the conditions that processing is necessary and done with equivalent secrecy. It is advisable under Articles 32.4, 28.3 and 39.1 of the Regulation that all staff is informed about the duty of secrecy and signs a binding confidentiality agreement. Nonetheless, the duty of

secrecy is closely linked with privacy. Furthermore, although for some professionals in healthcare and clinical research there are no obligations of professional confidentiality under national law or other rules, the effective exercise of the subject's autonomy requires all involved professionals to keep all information confidential.

The GDPR has expanded, as discussed earlier, the cases, under which health data could be processed. Article 9.2 (h) allows sensitive data processing when it "*is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3*". Furthermore Article 9.2 (i) permits processing "*for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy".* These two provisions establish legal grounds for regulatory uses of health data in health and pharmaceutical sectors, but also allow providers of social care to share health data under certain requirements. Recitals 53 and 54 require obligations of confidentiality as additional safeguards as to protect the rights and freedoms of natural persons. Recital 54 clarifies that "*such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies*".

Automated decision taking, including profiling, based on sensitive data is prohibited and can only be made under explicit consent or under EU or Member State law for reasons of *substantial public interest* grounds according to Article 4.4 and Recitals 71 and 72 of the new Regulation. *Substantial public interest* includes both public health and social security. It must be presented by the Member State under the principle of proportionality.

Electronic health records must be handling with precaution. The recipients of information in EHR are numerous: private Hospitals and Clinics, private doctors,

physiotherapists, occupational therapists, speech therapists, social workers psychologists, pharmacists, nurses, diagnostic imaging services, laboratories, administrative staff, and other health care providers. Also in these records other staff may have access such as the software company that provided and regularly maintains the EHR system .All data in EHR are sensitive and all professionals, who have access to these data, must comply with the GDPR.

In the case of *Avilkina and Others v. Russia* ECtHR held that the element of social need to protect public health was missing and there had been a violation of right to respect for private and family life[104]. The applicants were a religious organization and they complaint about the disclosure of their medical files to the Russian prosecution authorities after they refused to have blood transfusions during their stay in public hospitals.

Employment law and health data

According to both the Data Protection Directive and the GDPR there must be lawful grounds for processing information about an employee's health as these data are sensitive. As outlined earlier the processing of medical data must follow the requirements set out by Article 9 of the new Regulation. In European Union there are various employment laws where occupational medicine as a form of preventive medicine in the employment context exists[105]. Moreover, the nature of the job may require medical examination of the employee in order to determine his suitability for the particular work or in order to grant certain social benefits. In these cases health data must be collected exclusively from the employee concerned except if the employee has given explicit and informed consent or when the national law provides for it.

The collection of health data when data subjects must undergo medical examinations is regarded also very sensitive. These medical examinations may have the form of:

- drugs and alcohol tests

[104] Case of Avilkina and others v. Russia (Application No. 1585/09) Judgment 6 June 2013
[105] Frank Hendrickx ,(2002),"Protection of workers' personal data in the European Union", http://ec.europa.eu/social/BlobServlet?docId=2507&langId=en

- HIV test
- Genetic Tests[106]

In all the above medical examinations the legal basis for the processing is important. Legal bases could include the performance of a contract; comply with legal obligations, or the employer's legitimate interests. For special categories of data, the GDPR provides for when it is "*necessary for the purposes of carrying out the obligations and exercising the specific rights of the Controller or of the data subject in the field of employment law*"[107].

The lawful grounds often overlap. There are in the Strasburg jurisprudence cases that have dealt with employees and the protection of their personal data. In the case WRETLUND v. Sweden[108] the applicant was an office cleaner at a nuclear plant. She complained that her obligation to undergo a drug testing interfered with her right to respect for her private life under Article 8.1 of the ECHR. The Court decided that since the applicant was informed of the particular drug testing, this test was in accordance with the law and declared the application inadmissible. Another important case was about the HIV test. In the case of I.B. v. Greece[109] I.B was forced to undergo a HIV test in response to pressure from other employees and later he was dismissed from his job. ECtHR considered that the applicant was a victim of discrimination on account to his health status and there was a violation of Article 8(right to private life) and Article 14 (prohibition of discrimination) of the ECHR.

6.4 Health Data and New Technologies

The Article 29 Data Protection Working Party published letters[110][111] regarding the framework of the Commission's mHealth[112] and eHealth[113] initiative to clarify the

[106] Genetic testing is the use of laboratory tests to determine the genetic status of an individual.
[107] Art.9.2 (b) of GDPR, see also Article 8.2(b) of the Directive 95/46
[108] Inga-Lill Wretlund v. Sweden, (Application no. 46210/99, 09/03/2004)
[109] Case of I.B. v. Greece, (Application No. 552/10), Judgment, 3 October 2013
[110] https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf
[111] Letter of the Chair of the ART 29 WP to eHealth, 11th April 2018
[112] European Commission , (2014) *GREEN PAPER on mobile Health* ("mHealth"), Brussels,

definition of data concerning health in relation to lifestyle and wellbeing apps. "*Mobile health* (hereafter "mHealth")" covers "*medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices*"[114]

In a paper[115] and an annex[116] on health data in apps and devices, the Working Party supports a broad definition of health data, separating health data in three categories as regards the mobile devices:

1. The data are inherently/clearly medical data, when they are processed via the app or the device.
2. The data are raw sensor data that can be use via the app or in combination with other data to draw conclusions about the person's actual health status or health risk.
3. Conclusions are drawn, based on the data collected via the app or the device about an individual's health status or health risk (irrespective of whether these conclusions are accurate, legitimate or otherwise adequate or inadequate).

Information derived from the examination of a body part or bodily substance (e.g. blood pressure, heart rate e.t.c) information about disease risks (e.g. alcohol consumption) and information about the actual physiological or biomedical state of an individual also constitute health data according to Article 29 Working Party.

Furthermore, a grey area exist, as the Working Party states: "*If seemingly innocuous raw data are tracked over a period of time, combined with other data, or transferred to other parties who have access to additional complementary datasets, it may well be that even the seemingly most innocuous data, combined with other data sources, and used for other purposes, will come within the definition of 'health data'*."

---

[113] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century, Brussels, 6.12.2012

[114] European Commission , (2014) GREEN PAPER on mobile Health ("mHealth"), Brussels,

[115] ARTICLE 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices", Adopted on 27 February 2013

[116] ARTICLE 29 Data Protection Working Party , ANNEX - health data in apps and devices, https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_annex_en.pdf

The Working Party considers explicit consent as the most likely legal ground for processing health data. Health data processing via apps and devices requires, in line with the principle of transparency, that data Controllers clearly inform users "*whether the data are protected by any medical secrecy rules or not*."

The Commission has published, in addition, a Staff Working Document[117] which examines the EU legal framework that applies in lifestyle and wellbeing apps. In brief, the Document states that under the previous Directive 95/46/EC:

- If the data is transmitted outside the device then it is qualified as health data. Explicit consent will be required in any event of wellbeing or lifestyle app or device processes of location data or other data collected through sensors of the mobile device.
- Application and device developers must observe the data privacy rules
- The Directive does not apply when the lifestyle and wellbeing apps do not transmit outside the user's device.

7 Scientific Research in health

Big data have a key role in clinical research, but simultaneously create new challenges for data security and privacy. Machine learning is besides developing into one of the primary methods in clinical research, bringing new challenges to privacy and data security. Clinical research data are sensitive data although their processing is crucial for scientific or research purposes and play a key role in discovering new treatments. Clinical researchers must recognize the sensitive data that they process; the purposes it is used for, the persons that have access to it and guarantee all employees are informed and trained to protect them. Moreover, in Biobanks technical details regarding cells and tissue samples, personal information about sample donors, and research datasets are generated from the use of human bioresources. Balancing

[117]European Commission, (2014) "Commission staff working document on the existing EU legal framework applicable to lifestyle and wellbeing apps Accompanying the document GREEN PAPER on mobile Health ("mHealth)", Brussels,

the need to protect the privacy of individual donors or research participants with the facilitation of effective research is an ongoing challenge.

The new EU General Data Protection Regulation, while aiming to provide better safeguards for individuals' personal data may also have significant implications for data protection practices of researchers, industry, and Biobanks around the globe. The aim is to balance privacy with innovative medical research.

7.1 Rules for clinical research and clinical trial under GDPR

According to Article 4 in paragraph 13 of the new Regulation 2016/679 (GDPR) genetic data is "*personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*" and in Recital 34 there is a definition "*Genetic data should be defined as personal data relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained*". The analysis of the biological sample is considered to be data, but not the sample itself. The sample is thus not protected under EU Data Protection Law[118]. The GDPR defines biometric data as "*personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person*".

Clinical research is a medical research undertaken in humans. *Clinical trials,* which fall under the umbrella of clinical research specifically, are experiments or observations conducted and are linked to clinical research[119]. Biomedical or behavioral research studies on human participants are designed to analyze biomedical or

[118] Jane Reichel, (2017), "Oversight of EU medical data transfers an administrative law perspective on cross-border biomedical research administration", *Health and Technology*, December 2017,Volume 7, Issue 4, pp 389–400

[119] https://grants.nih.gov/policy/clinical-trials/definition.html

behavioral interventions, including new treatments (such as vaccines, drugs, dietary supplements, and medical devices), known treatments that need additional revision and evaluation and compare new drugs negative and positive effects and efficacy to older drugs. An ethics committee approval is obligatory in order for a clinical trial to begin[120]. These committees have the competency for evaluating the risk and benefit proportion of the trial. Depending on product type and development stage, researchers initially enroll volunteers or patients into small pilot studies, and subsequently conduct progressively larger scale comparative studies[121]. Clinical trials can vary in size and cost, and they can involve a single research center or multiple centers, in one country or in multiple countries.

The current regime that applies in clinical trials in the EU is the Directive 2001/20/EC[122]. The new Clinical Trial Regulation No 536/2014[123] will come into application probably in 2019. The timing of its application depends on the development of a fully functional EU portal and database by the European Medicines Agency together with the EU countries and the Commission[124]. The Regulation harmonises the assessment and supervision processes for clinical trials throughout the EU, via an EU portal and database. Until the Clinical Trials Regulation EU No 536/2014 will become applicable, all clinical trials performed in the European Union are required to be conducted in accordance with the Clinical Trials Directive. This Directive will be repealed on the day of entry into application of the Clinical Trials Regulation. It will however still apply three years from that day to[125]:

- Clinical trials applications submitted before the entry into application

[120] According to the *Declaration of Helsinki* issued by the World Medical Association, research on human should be clearly formulated in experimental protocols and these should be submitted to independent ethical review boards (ethics committees and institutional review boards) for approval. (2000) http://www.wma.net/e/policy/b3.html

[121] Elizabeth de Poy,(2017) Introduction to Research, Understanding and Applying Multiple Strategies, 4th Edition, Just the facts 101, Textbook Key Facts, Context Technology Inc,

[122] DIRECTIVE 2001/20/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 April 2001 on the approximation of the laws, regulations and administrative provisions of the Member States relating to the implementation of good clinical practice in the conduct of clinical trials on medicinal products for human use

[123] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC

[124] https://ec.europa.eu/health/human-use/clinical-trials_en

[125] Ibid.

- Clinical trials applications submitted within one year after the entry into application, if the sponsor opted for the old system.

The new Regulation No 536/2014 will strengthen transparency of trial information, efficacy of clinical trials and safety of the subjects. The scope of the Regulation No 536/2014 is extensive but as regards to the personal data of the persons participating in a clinical trial the Regulation requires informed consent and states that by law, all information entered in the clinical trial database is publicly accessible, except personally identifiable information, commercially confidential information, and confidential communication between and among member states[126]. The legislation of Member States where patients are located may differ, so it is essential to ensure that explicit consent is appropriate for the type of data that is collected, mainly regarding genetic data if it is mandatory by the protocol.

Together with the new Regulation No 536/2014, GDPR stipulates in Recital 161 that "*for the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council[1] should apply*".

It is important to identify the key roles of the parties in a clinical study in order to determine the party that is responsible for compliance with the EU data protection rules, the applicable Member State law and how the data subjects can exercise their rights under GDPR. Under the Data Protection Directive, the data Controller (i.e. sponsor) is responsible for compliance with the rules. Under the GDPR, the concept of joint data Controllers is introduced, and obligations on data Processors are imposed.

The new Regulation No 536/2014 introduces co-sponsorship and non-commercial sponsorship in clinical trials in Article 72. Unless decided differently in a written binding contract, all Sponsors have the full responsibilities of a Sponsor as defined in the Regulation No 536/2014 and GDPR. Co-sponsors can *jointly establish* which Sponsor will serve as a contact point for receiving all questions from subjects, investigators, or Member States. The clinical trial Sponsor is responsible for determining whether the study must comply with the GDPR. If the trial is subject to the GDPR, detailed data privacy information, that the GDPR requires, must be provided

[126] "Regulation EU No 536/2014: What's New and What's Changed" http://pharm-olam.com

to all the participants. In clinical research the Sponsor is a Controller. Other entities may act as joint[127] Controllers (e.g. an investigator in a clinical trial). Anyone appointed by the Sponsor to work with the clinical trial, such as personnel, sales, and sub-contractors e.t.c is a data Processor. Organisations that process and manage clinical trial data should carry out data impact assessments (DIA) because sensitive data processing "*is likely to result in a high risk to the rights and freedoms of natural persons*"[128]. A data impact assessment (DIA) must include identification of the need for a DIA, description of the information flow, identification of the data processing and related risks, description of solutions to reduce or eliminate these risks, the outcomes of the DIA and integration of the data protection solutions into the clinical trial. Moreover, the Controller will have to consult the supervisory authority in the cases where Member State law obliges Controllers to consult with, and/or take prior authorisation from the competent supervisory authority especially when the processing is referring to public health according to Article 36.5 of the GDPR.

The Article 29 Working Party has published a useful guide of what kind of processing is likely to result in a high risk of rights and freedoms and gives direction on how a DIA is carried out[129]. According to Article 29 Working party an impact assessment "*should be continuously carried out on existing processing activities*" and "*should be re-assessed after 3 years, perhaps sooner, depending on the nature of the processing and the rate of change in the processing operation and general circumstances*"[130]. In addition, according to Article 37 of the Regulation 2016/679 the appointment of a Data Protection Officer is mandatory where "*the core activities of the Controller or the Processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale;*" or when "*the core activities of the Controller or the Processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in*

[127] Article 26 of the GDPR
[128] Article 35 of the GDPR
[129] ARTICLE 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679" Adopted on 4 April 2017
[130] Ibid. p. 12

Article 10". Consequently, a Data Protection Officer should be designated when sensitive data are being processed in clinical researches and trials.

If clinical trials are conducted outside the EU, but submitted for marketing authorisation in the EU, they have to follow similar principles to the provisions of the Clinical Trials Directive (Annex I, point 8 of the Directive 2001/83/). Article 3.1 of the GDPR states:

1. *This Regulation applies to the processing of personal data in the context of those activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

2. *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*

(a) *The offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*

(b) *The monitoring of their behavior as far as their behavior takes place within the Union.*

For example, if a medical researcher processes personal data in US and uses a data storage service established in the EU, then the US medical researcher is a Controller and the data storage service is a Processor. The US medical researcher as a Controller must adhere to EU law in regards to the data stored with the European service provider.

GDPR clearly states in Articles 17 and 20 that data subjects have the right to erase or transfer their data. In a clinical research this may be challenging. Clinical data if removed or transferred from a dataset, may result in altering the audit trail or the statistical outcome. How the science community will respond to such challenges is a matter yet not resolved. Subjects can, nevertheless, withdraw their consent to prevent any additional data collection or exercise their other rights under GDPR.

Furthermore, Article 12 of the Medical Data Recommendation[131] [132]regulates scientific research. The provision requires that medical data used in scientific research

[131] Council of Europe, Committee of Ministers, Recommendation (1997) No. R (97) 5 on the Protection of Medical Data.

[132] Article *12.* of the Recommendation No R (97) 5

shall be anonymised. In addition, it advices professionals and scientific organisations to implement techniques and procedures to ensure anonymity. It is, however, possible to use personal data if the research pursues a legitimate aim and is impossible to continue the research without this data. These conditions should apply:

1. The data subject or the legal representative of an incapacitated data subject has provided informed consent.
2. The research serves high public interests and it is authorised by the responsible national agency.

Scientific research

12.1. Whenever possible, medical data used for scientific research purposes should be anonymous. Professional and scientific organisations as well as public authorities should promote the development of techniques and procedures securing anonymity.

12.2. However, if such anonymisation would make a scientific research project impossible, and the project is to be carried out for legitimate purposes, it could be carried out with personal data on condition that:

a. the data subject has given his/her informed consent for one or more research purposes; or

b. when the data subject is a legally incapacitated person incapable of free decision, and domestic law does not permit the data subject to act on his/her own behalf, his/her legal representative or an authority, or any person or body provided for by law, has given his/her consent in the framework of a research project related to the medical condition or illness of the data subject; or

c. disclosure of data for the purpose of a defined scientific research project concerning an important public interest has been authorised by the body or bodies designated by domestic law, but only if:

i. the data subject has not expressly opposed disclosure; and

ii. despite reasonable efforts, it would be impracticable to contact the data subject to seek his consent; and

iii. The interests of the research project justify the authorisation; or

d. the scientific research is provided for by law and constitutes a necessary measure for public health reasons.

12.3. Subject to complementary provisions determined by domestic law, health-care professionals entitled to carry out their own medical research should be able to use the medical data which they hold as long as the data subject has been informed of this possibility and has not objected.

12.4. As regards any scientific research based on personal data, the incidental problems, including those of an ethical and scientific nature, raised by respect of the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data should also be examined in the light of other relevant instruments.

12.5. Personal data used for scientific research may not be published in a form which enables the data subjects to be identified, unless they have given their consent for the publication and publication is permitted by domestic law.

3. The scientific research is provided for by law and constitutes a necessary measure for public reasons.

Article 29 Working Party has expressed similar opinion about the matter[133]. In the Opinion the Working Party is concerned about the status of pseudonymous data in the context of research. Specifically, it states in the Opinion that: "*Retraceably pseudonymised data may be considered as information on individuals which are indirectly identifiable. Indeed, using a pseudonym means that it is possible to backtrack to the individual, so that the individual's identity can be discovered, but then only under predefined circumstances. In that case, although data protection rules apply, the risks at stake for the individuals with regard to the processing of such indirectly identifiable information will most often be low, so that the application of these rules will justifiably be more flexible than if information on directly identifiable individuals were processed", "identified or identifiable" – focuses on the conditions under which an individual should be considered as "identifiable", and especially on "the means likely reasonably to be used" by the controller or by any other person to identify that person. The particular context and circumstances of a specific case play an important role in this analysis. The opinion also deals with "pseudonymised data" and the use of "key-coded data" in statistical or pharmaceutical research.*

Under the GDPR, as mentioned before, pseudonymised data are personal data and have to be protected accordingly. Confidentiality and data security provisions must be applied to sensitive data processing in the context of clinical trials. Besides pseudonymisation, other safeguards (such as encryption) will need to be considered and implemented as well according to recital 28. For clinical research projects not based on informed consent, like observational studies, the Controller must apply the suitable safeguards according to Article 89 of the Regulation. While the GDPR was in its development, the Medical Science Committee[134] and other commentators were concerned about possible negative implications pseudonymised data will have for

[133] ARTICLE 29 Data Protection Working Party "Opinion 4/2007 on the concept of personal data" Adopted on 20th June 2007

[134] Medical Sciences Committee, (2013), Opinion Paper "The Benefits of Personal Data Processing for Medical Sciences in the Context of Protection of Patient Privacy and Safety"

research[135]. According to its Opinion, the MED Committee suggested adoption of a risk-managed approach in the case of pseudonymised data since there are appropriate technical safeguards in the research field that reduce the risk of re-identification otherwise*, "many research projects will become unmanageable and the ability to respond rapidly to medical questions of importance will be limited"*.

Article 9 of GDPR, prohibits processing unless certain conditions are met. In Article 9.2.(j) is defined that if the "processing is necessary for archiving purposes in the public interest, scientific or historical *research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*" then the processing is allowed. Article 89, states that "*Where personal data are processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfillment of those purposes*." Scientific research according to Recital 159 of the GDPR should be interpreted broadly and it provides some examples of what may constitute scientific research. The recital makes a reference to Article 179.1 of the Treaty on the Functioning of the European Union, which endorses "*the objective of strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely*."It is yet ambiguous if the Regulation requires the research to be published, as the Treaty states in order to fall in the scientific research concept. . Even so, GDPR prioritizes research in order to foster innovation combined with adequate security measures to protect personal data. The Directive permitted secondary processing for research purposes provided that the Member States had "furnished suitable safeguards"[136]. Accordingly, the Controller was not allowed to

[135] Stevens, L 2015, 'The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK' *European Data Protection Law Review*, vol. 1, no. 2, pp. 97-112.
[136] Recital 29 of EU Directive 95-46-EC

further process personal data outside the purposes for which it was collected, except when the member state had endorsed legislation permitting processing activities for research purposes. The GDPR makes an exception to the principle of purpose limitation for research. Article 5.1 defines that, "*further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes."*

Article 6.4 of the GDPR entails that further process of sensitive data for a purpose that involves research is permissible even though research was not the purpose for the initial collection. Recital 50 of the GDPR states that further processing is permissible when the secondary processing is "*compatible*," such as for research Compatibility is examined according to Article 6.4 in relation to "*the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9*". On the other hand, under the previous Directive, "*further processing of personal data concerning health, data about children, other vulnerable individuals, or other highly sensitive information should, in principle, be permitted only with the consent of the data subject*".[137]

Article 8 of the GDPR includes specific provisions for the processing of children's data so Sponsors are required to make "*reasonable effort*" to ensure that the parent or guardian has provided valid consent if the clinical trial includes children.

7.2 Biomedical research and Biobanks

The enactment of GDPR will affect directly biomedical research in many ways. More specifically Biobanks and research organisations must comply with the Regulation in order to lawfully continue their research progress and simultaneously protect the data subjects' personal and sensitive information.

Cell based research especially iPSC research requires all involved parties to comply with the GDPR. Induced pluripotent stem cells (iPSC) are a type of pluripotent stem cell that can be generated directly from adult cells. iPSC can be derived directly from adult tissues and can be made in a patient-matched manner, which means that

[137] Article 29 Working Party, Opinion 08/2001

each individual could have their own pluripotent stem cell line. iPSCs are used in personalized drug discovery efforts and understanding the patient-specific basis of disease[138]. The technology of iPSC is currently widely used and has very prominent results. When the iPSC is derived from fetal tissue or from a diseased donor then the Regulation about the protection of personal data is not applied. Nonetheless, if the method is applied in living donors these individual's sensitive personal data require legal protection. The GDPR concerns iPSC that are derived from new donated material or existing tissue samples that are not fully anonymous, but pseudonymised[139]. The use of human biological material for cell-based research and clinical interventions has many risks to the privacy of patients and donors since these stem cell lines hold extensive genetic characteristics of the parent/donor somatic cell or tissue. This poses high risks in privacy protection is the possibility of re-identification of individuals from anonymised cell lines and associated genetic data[140].

In order to minimize the risk to privacy of the donors/patients, valid consent should contain all the necessary information required by the Regulation and certainly the purposes the biological sample is collected, can be reprogrammed, can be stored and can be shared together with the personal and/or medical data of the participant. In order to later derive human iPSC from tissue samples that were obtained previously in support of a research plan that did not include iPSC derivation, a new consent for the data processing new purpose must be obtained according to GDPR and the purpose limitation principle, if it is not compatible with the research purpose. It is worth noting that Article 6.4 of the GDPR allows for subsequent processing operations that are "compatible." Moreover, in Recital 50 it defines that further processing for research purposes "should be considered to be compatible." The previous Data Protection Directive defined in Recital 29 that secondary processing for research purposes was permissible only if the Member States had the necessary "suitable

[138] Takahashi, K; Yamanaka, S, (2006), "Induction of pluripotent stem cells from mouse embryonic and adult fibroblast cultures by defined factors". *Cell*, 126 (4): 663–76.

[139] Michael Morrison, Jessica Bell, Carol George, Shawn Harmon, Megan Munsie & Jane Kaye, (2017), "The European General Data Protection Regulation: challenges and considerations for iPSC researchers and Biobanks", *Regenerative Medicine*, Vol. 12, No 6.

[140] Ogbogu U, Burningham S, Ollenberger A et al. (2014), " Policy recommendations for addressing privacy challenges associated with cell-based research and interventions". *BMC Med. Ethics* 15, 7, Reports on a multidisciplinary workshop on how to best manage privacy issues associated with cell-based research

safeguards" .Hence, the Controller could not process personal data further than the purposes for which it was collected, except when the Member State had enacted legislation allowing these kind of processing activities for research purposes.

It is obligatory under GDPR to ensure that data subjects understand and consent to all the information about how the data will be used and distributed[141], so health professionals should ensure that participants give permission to share cell lines and data with researchers in other countries, the private sector and consent to post-study deposition of the lines and data in a biobank such as EBiSC[142]. iPSC researchers who generate cell lines and collect clinical data must find and apply, in order to ensure a long-term research plan, stable means of access to the pseudonymisation key that links individual donors and their samples/data[143]. For Biobanks and research groups who produce and share human iPSC, part of the competences of the designated Data Protection Officer could be the responsibility for the protection of the pseudonymisation keys, and the competency, as a contact point, to examine traceability and re-contact requests[144].

A biobank is a type of biological materials repository that collects, processes, stores, and distributes biospecimens, usually human's to support future scientific investigation and for use in research. Biobanks give researchers access to data representing a large number of people. Samples in Biobanks and the data derived from those samples can often be used by multiple researchers for cross purpose research studies[145].

The core activities of Biobanks are processing operations that entail regular and systematic monitoring of the data subjects on a large scale, consequently a Data Protection Officer must be appointed by the Biobank Controller or the Processor in order to assist, monitor and guarantee internal compliance with GDPR. A Data Privacy Impact Assessment is also required for the processing of sensitive data by a Biobank.

[141] Ibid.
[142] Lomax GP, Chandros HS, Rosario I. (2015), "The DISCUSS project: revised points to consider for the derivation of induced pluripotent stem cell lines from previously collected research specimens", *Stem Cells Transl. Med***.** 4(2), 123–129
[143] Michael Morrison, Jessica Bell, Carol George, Shawn Harmon, Megan Munsie & Jane Kaye, (2017), "The European General Data Protection Regulation: challenges and considerations for iPSC researchers and Biobanks", *Regenerative Medicine*, Vol. 12, No 6
[144] Ibid.
[145] Greely, H. T. (2007). "The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks". Annual Review of Genomics and Human, *Genetics*, 8: 343–364.

Participants should also be informed, in the informed consent framework, about what data will be shared. Research involving genetic data and next-generation sequencing data may lead to concerns about (i) whether data can identify individuals and/or family members, and (ii) whether to return results from this type of analysis[146].

7.3 Secondary use of health data

Secondary use of health data provides personal health information for research applications usually after the direct health care. A substantial amount of information is collected throughout the provision of care and treatment, some of it specific to the patient being treated, some of it not. The use of electronic medical records made the mass collection of public health data possible. Secondary use must be performed under professional and legal obligations of confidentiality. Practically, secondary use of data is applied in order to:

- Advance the quality of clinical care
- Protect public health by monitoring and responding to infectious diseases and other environmental hazards
- Improve the management of the health system,
- Ensure that health policy is evidence-based through carrying out empirical research
- Provide better information to the public about healthy lifestyles
- Process large amounts of data from multiple sources
- Research by others using data collected by the care team without being a part of it
- Research which requires further contact with patients or former patients[147].
-

The benefits from the secondary use of information are important. The health of the population may be improved by actions such as disease surveillance, screening and needs assessment and preventive activities. It is also significant for clinical and

[147] Joint Action to support the eHealth Network, REPORT on How to handle health data for purposes other than patient care", For discussion to the members of the eHealth 11th meeting on 09 May 2017

medicine safety when evaluating long term effects of drugs and treatments. On the other hand, unauthorized disclosure of personal health or genetic information could have a negatively impact on a patient's personal and professional life. Ethical concerns about secondary use of data most frequently revolve around potential harm to individual data subjects. Re-use of sensitive data personal data requires always very careful consideration.

The principles of handling personal data are important in secondary use of health data. These have been embedded in the General Data Protection Regulation. It must be emphasized that all the principles apply regardless of whether there is a "primary" or "secondary" use of data. Purpose can be problematic if the secondary use was not anticipated and the subject did not give his or her informed consent when the data was collected. The application of the process and the standards will typically require specific consideration of individual systems and data check flows. A Data Privacy Impact Assessment (DIA) and the designation of a DPO will minimize the risk of breaches in personal health data.

7.4 Incidental findings-subject's information

Incidental findings are a major ethical dilemma in medical research. Participants must be given an informed consent form and detailed information sheets that: state what procedures will be implemented in the event of unexpected or incidental findings (in particular, whether the participants have the right to know, or not to know, about any such findings)[148]. As genetic knowledge increases, it is now feasible to identify a variety of genetic findings for most participants unrelated to the primary focus of the study. In the context of genetic testing, the "right not to know" is the concept that any individual should be permitted to control whether they receive genetic information—particularly information about the risk of future illness—and that their desire not to know certain kinds of information should be respected. The justifications for a right

[148] EUROPEAN COMMISSION Directorate-General for Research & Innovation Horizon 2020 Programme Guidance, "How to complete your ethics self-assessment" 23 July 2018,

not to know are grounded in respect for decisional autonomy and/or an interest in protecting individuals from receiving unwanted and potentially harmful information[149].

Conversely, there are many challenges in the consent process. Researchers will not know the likely findings for any specific participant or donor. Thus, the benefits and risks of receiving such data and other relevant information will need to be framed in general terms. Informed consent must, furthermore evaluate the effect on the patient's family, because, for example genetics is linked to heredity and filiation and his or her right to autonomy in relation to incidental findings .In any case the decision of whether the incidental findings will be disclosed rests only with the involved data subject.

7.5 Data Transfers

The GDPR preserve requirements for data transfers outside the EU. Article 44 of the General Data Protection Regulation sets out the general principles for allowing transfers to third countries, including any onward transfer, "*Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation*".

The Data Protection Directive had a broad definition of territorial scope[150], and the General Data Protection Regulation expands it even further. EU data protection law has a general position that the rights of EU data subjects should be protected regardless of where the data is processed. Such transfers occur, for example, when persons located in the US have access to data stored in the EU. When personal data collected in the EU is transferred to another country outside the protection of the Regulation, important restrictions apply. Moreover, special categories of data, such as

[149] Benjamin E. Berkman and Sara Chandros Hull, (2014), "The "Right Not to Know" in the Genomic Era: Time to Break From Tradition?" *Am J Bioeth*. 2014 Mar; 14(3): 28–31.
[150] Article 4 of the Data Protection Directive

health data, there must further be a specific legal ground for processing. The Regulation provides for three requirements for a transfer of data outside EU:

1. The Commission has enacted an *adequacy decision* about the adequate level of the legal framework of data privacy in a country, a territory or one or more specified sectors within that country according to Article 45 of the GDPR.
2. Data may be transferred if *appropriate safeguards* are available, on the condition that enforceable data subject rights and effective legal remedies for data subjects are available according to Article 46 of the new Regulation.
3. Article 49 sets out derogations in the absence of the aforementioned adequacy decision or appropriate safeguards. That are the existence of an explicit informed consent from the data subject where he or she has been informed of the possible risk of transfer, the transfer is necessary due to a contract involving the data subject, an important reason of public interest or in connection to a legal claim, the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent, the transfer is made from a register which according to Union or Member State law is intended to provide information to the public. Moreover, according to Article 49 "*where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued".*

The Safe Harbor Agreement (SHA)[151] was a set of principles drafted in the year 2000 and an example of adequacy decision under the Data Protection Directive that governed the transfer of user data from the European Union and Switzerland to the United States. It was ruled invalid by the European Court of Justice in October 2015. Safe Harbor included seven principles of notice, choice, onward transfer, security, access, integrity and enforcement. The agreement itself was annexed to an actual decision enacted by the Commission. US importers have to comply with these principles, to publicly certify their compliance with the US Department of Commerce and subject themselves to enforcement by the US Federal Trade Commission to the extent their certification materially misrepresented any aspect of their processing of personal data imported from Europe[152]. One of the most important data privacy cases arose from a complaint against Facebook brought to the Irish Data Protection Commissioner by an Austrian privacy advocate named Max Schrems. In the complaint, Mr. Schrems challenged the transfer of his data and the data of EU citizens to the United States by Facebook, which is incorporated in Ireland. The case was brought before the Court of Justice of the European Union and on October 6, 2015 CJEU invalidated the Safe Harbor arrangement, which governed data transfers between the EU and the US[153]. A new adequacy decision, after the CJEU invalidation, the EU-US Privacy Shield[154], was enacted in July 2016 .The Privacy Principles of the EU-US Privacy Shield included thirteen Framework Principles similar to those in the Safe Harbor-agreement. The agreement also includes Supplemental Principles.

Transfer of data within medical research from the EU must comply with the requirements set out by the Regulation. The principles that are enshrined in Safe Harbor, the Schrems-case and EU-US Privacy Shield are important for medical

[151] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce

[152] Aaron P Simpson, Hunton & Williams, “Safe Harbour and the Privacy Shield”, 06 September 2017, published online, https://gettingthedealthrough.com

[153] "Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid" Court of Justice of the European Union. 6 October 2015.

[154] Commission implementing decision of 12.7.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, C (2016) 4176 final (EU/US Privacy Shield Decision)

research, as they present a standard level of protection that EU data subjects must enjoy.

Conclusions

GDPR is a challenging Regulation. It brings additional protection of personal data but also raises issues that will need time to overcome in order to fully implement all the changes that it requires.

GDPR has directly affected data privacy and security standards while in addition indirectly drives all organisations that keep and process personal data to develop and improve their cyber security measures, in order to avoid any potential data breach. Furthermore, Data Protection Agencies from each Member State evaluate GDPR compliance consequently the Regulation standardized throughout EU the regulatory environment.

In health and sensitive data in general, the GDPR provides to every patient the opportunity to gain more control over the personal data that is being collected and processed about them, as well as the purposes the data are used. One of the core components of the GDPR, the purpose and the location of any data that's collected, ensures that healthcare providers will have a more detailed examination of their patients, which could direct to improved, and more correct diagnosis, as well as more targeted treatments.

The recent incidents in data breaches are evident of the need for enhanced protection. Cambridge Analytica in March 2018 was reported to illegally sourced Facebook data and used them to influence a variety of political campaigns. The personal data of approximately 87 million Facebook users were acquired, without their knowledge and their consent[155]. In 2017 the WannaCry cyber attack[156] affected multiple organisations including healthcare services like National Health Services hospitals in England and Scotland and was unprecedented in scale.[157]

[155] https://en.wikipedia.org/wiki/Cambridge_Analytica

[156] WannaCry is a ransomware cryptoworm, affecting computers with the Microsoft Windows operating system

[157] https://www.reuters.com

On the other hand, departure from the rules of the GDPR in sensitive data processing, must take place only when the public interest undoubtedly prevails over a corresponding right in protecting and preserving individual privacy and autonomy. The rationale must be clearly and specifically demonstrated, and balanced against actual evidence of consequent benefits and risks. Especially in health data and clinical research the balance must be case-specific evaluated , and should be implemented by a body or institution that is familiar with, or structured to obtain and incorporate into its deliberative and decision-making process, multiple perspectives on the research context, associated privacy challenges[158]. Cross-border research involving human biological material that contains identifiable genetic information about a research participant requires harmonization with other non EU jurisdictions in order to be facilitated and provide reliable outcomes without the breach of the Regulation. Some of the requirements of GDPR are relatively easily addressed by putting in place data protection policies for all clinical research involving humans. Other prerequisites of the GDPR probably will increase the bureaucratic burden of sharing, at least on a large scale, human derived iPSC cells and data and will require additional administrative support such as the appointment of specialist Data Protection Officer and the constantly assessment and revision of a DIA. In biobanking data minimization and transfer of samples outside Europe also will be potentially the most challenging development[159].A move toward digital tools for consent and engagement may offset some of the administrative burden of sustained interaction[160]. Concurrently, the retention of quality, safety, data protection, traceability and other GDPR conditions is likely to result in high running costs for Biobanks. To meet these costs cell banks may have to leverage the value of well-characterized iPSC to the pharmaceutical industry through longer term engagement between public and private sectors[161]. A possible failure to comply with the rules of GDPR may result not only in restraining research

[158] Kerina H. Jones et al. (2016)"The other side of the coin: Harm due to the non-use of health-related data", *International Journal of Medical Informatics,* 22 September 2016

[159] Teare HJA, Morrison M, Whitley EA, Kaye J. (2015) Towards 'Engagement 2.0': Insights from a study of dynamic consent with biobank participants. *Digital Health* 1, 1–13

[160] Kaye J, Whitley EA, Lund D, Morrison M, Teare H, Melham K. (2014) "Dynamic consent: a patient interface for twenty-first century research networks" *Eur. J. Hum. Genet.* 23, 141–146

[161] Ogbogu et al. (2014) "Policy recommendations for addressing privacy challenges associated with cell-based research and interventions" *BMC Medical* (Tom Huskinson, 2016)*Ethics* 15:7

development using iPSC but in hitting the public trust and support for this significant aspect of medical research.

Moreover, harm due to the exclusion of health data usage, or data non-use, is a matter that needs attention. The large administrative process and the complicated requirements of GDPR on data access perhaps will result in non usage of health data. Also, it can be argued that, in some cases the pursuit of informed consent can disadvantage certain groups, particularly those who are hard to reach or are on the edges of society[162].

Reaching the most advantageous balance is challenging and unlikely to be stable over time. The balance must protect individual right in medical data protection in accordance with the promotion of innovation in clinical research.

.

[162] Tom Huskinson, Nicholas Gilby, Harry Evans, Jane Stevens, and Sarah Tipping (2016) Wellcome Trust, Summary Report Wave 3: Tracking "Public Views on Science and Biomedical Research".

8 Bibliography

1. *Consolidated text of the modernisation proposals of Convention 108 finalised by the CAHDATA, Meeting of 15-16 June 2016,* (2016).
2. *Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS 108 (Explanatory Report to Convention 108),* (1981).
3. *Directive (EU) 2016/680, entered into force in 5 May 2018*, (2016).
4. Aaron P Simpson, H. &. (2017, September 6). *Getting the deal through.* Retrieved November 2, 2018, from Safe Harbour and the Privacy Shield: https://www.gettingthedealthrough.com
5. ARTICLE 29 DATA PROTECTION WORKING PARTY ,17/EN WP 258 "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680") . (2017, November 2017).
6. ARTICLE 29 Data Protection Working Party "Opinion 4/2007 on the concept of personal data" . (2007, June 2007).
7. ARTICLE 29 DATA PROTECTION WORKING PARTY, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679". (2017, October 17).
8. ARTICLE 29 Data Protection Working Party, "Guidelines on the right to data portability" . (2016, December 13).
9. ARTICLE 29 DATA PROTECTION WORKING PARTY, "Guidelines on transparency under Regulation 2016/679", . (2018, April 11).
10. ARTICLE 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices". (2013, February 23).
11. ARTICLE 29 Data Protection Working Party, "Working Document on the processing of personal data relating to health in electronic health records (EHR)". (2007, February 15).
12. *Article 29 Working Party .* (2013, February 27). Retrieved November 1, 2018, from Annex 2 Proposals for Amendments regarding exemption for personal or household activities : https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf
13. Article 29 Working Party Guidelines on consent under Regulation 2016/679. (2018, April 10).
14. Article 29 Working Party Opinion 8/2010, "Opinion 8/2010 on applicable law" . (2010, December 16).
15. Article 29 Working Party Opinion 8/2010, "Opinion 8/2010 on applicable law" . (2016, December 16).
16. Benjamin E. Berkman, S. C. (2014, March). The "Right Not to Know" in the Genomic Era: Time to Break From Tradition? *Am J Bioeth* , pp. 14(3): 28–31.

17. Bennett, C. J. (1992). *REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES.* Ithaca and London: Cornell University Press.
18. Burkert, H. (2000). Privacy Data Protection. A German/European Perspective. In K. H. Christoph Engel, *Governance of Global Networks in the Light of Differing Local Values* (pp. 43--70). Baden-Baden: K. H. Keller.
19. COMMISSION STAFF WORKING DOCUMENT on the existing EU legal framework applicable to lifestyle and wellbeing apps Accompanying the document GREEN PAPER on mobile Health ("mHealth")", Brussels, . (2014, April 10).
20. *COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS "eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century".* (2012, December 06). Retrieved 11 2, 2018, from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52012DC0736
21. *Convention for the protection of Human Rights and Fundamental Freedoms*. (1951). Retrieved from www.coe.int
22. *Council of Europe*. (n.d.). Retrieved from Guidelines on the protection of individuals with regard to the processing of personal dta in a world of big data: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2015/20150205_letter_art29wp_ec_health_data_after_plenary_en.pdf
23. *Council of Europe*. (n.d.). Retrieved October 15, 2018, from https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/005
24. Council, E. P. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da.*
25. Directive 2001/20/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL . (2001, April 4).
26. et, K. H. (2016, September 22). The other side of the coin: Harm due to the non-use of health-related data. *International Journal of Medical Informatics* .
27. *EU Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law.* (2018). Luxembourg: Publications Office of the European Union.
28. European Commission, "GREEN PAPER on mobile Health ("mHealth")", Brussels, . (2014, April 10).
29. European Commission, Directorate-General for Research & Innovation. (2018, July 23). How to complete your ethics self-assessment. *Horizon 2020 Programme Guidance* .
30. European Commission. (2014). "Commission staff working document on the existing EU legal framework applicable to lifestyle and wellbeing apps . *Accompanying the document GREEN PAPER on mobile Health ("mHealth)"* . Brussels.
31. Explanatory Memorandum Recommendation No.R (97) 18 of the Committee of Ministers to Member States concerning the protection of personal data collected and processed for statistical purposes", . (1997, Semptember 30).

32. Flaherty, D. H. (1991). On the Utility of Constitutional Rights to Privacy and Data Protection. *Case Western Reserve Law Review* , p. 831.
33. Google Spain SL and Google Inc. against Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case number C-293/12 (Court of Justice of the European Union April 8, 2014).
34. Greely, H. T. (2007, September). The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks. *Annual Review of Genomics and Human, Genetics, 8* , pp. 343–364.
35. Greer, S. (1997). *The exceptions to Articles 8 to 11 of the European Convention on Human Rights.* Strasbourg Cedex: Printed at the Council of Europe.
36. *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data .* (2017, January 23). Retrieved from Council of Europe, Committee of Convention 108: https://rm.coe.int/16806ebe7a
37. Handbook on European data protection law, European Union Agency for Fundamental Rights, Council of Europe. (2014).
38. Judgment in Maximillian Schrems v Data Protection Commissioner: The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid, Case C-362/14 (Court of Justice of the European Union October 6, 2015).
39. Kaye J, W. E. (2014, May 7). Dynamic consent: a patient interface for twenty-first century research networks. *Eur. J. Hum. Genet. 23* , pp. 141–146.
40. Medical Sciences Committee. (2013). The Benefits of Personal Data Processing for Medical Sciences in the Context of Protection of Patient Privacy and Safety. *Opinion Paper* .
41. Morrison M., e. a. (2017, October 4). The European General Data Protection Regulation: challenges and considerations for iPSC researchers and Biobanks. *Regenerative Medicine, Vol. 12, No 6* , pp. 693-703.
42. Network, J. A. (2017). REPORT on How to handle health data for purposes other than patient care. *For discussion to the members of the eHealth 11th meeting on 09 May.*
43. *OECD* Retrieved October 16, 2018, https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf
44. Ogbogu Ubaka, e. a. (2014, February 3). Policy recommendations for addressing privacy challenges associated with cell-based research and interventions. *BMC Medical Ethics* .
45. *Pharm-Olam*. (2018). Retrieved from Regulation EU No 536/2014: What's New and What's Changed": http://pharm-olam.com
46. Plakiewicz, J. (2011). "Convention 108 as a global privacy standard?" . *International Data Protection Conference.* Budapest.
47. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling Adopted by the Committee of Ministers on 23 November 2010 at the. (n.d.).
48. Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC. (2014, April 16).

49. Reichel J. (2017, December). Oversight of EU medical data transfers an administrative law perspective on cross-border biomedical research administration. *Health and Technology, Volume 7, Issue 4* , pp. 389–400.
50. Stevens, L. (2015). The Proposed Data Protection Regulation and Its Potential Impact on Social Sciences Research in the UK. *European Data Protection Law Review vo.1, no. 2* , pp. 97-112.
51. Takahashi, K; Yamanaka, S. (2006). Induction of pluripotent stem cells from mouse embryonic and adult fibroblast cultures by defined factors. *Cell, 126 (4)* , pp. 663–76.
52. Teare HJA, M. M. (2015, August 2015). Towards 'Engagement 2.0': Insights from a study of dynamic consent with biobank participants. *Digital Health* , pp. 1–13.
53. The World Medical Association Declaration of Helsinki Recommendations guiding physicians in biomedical research involving human subjects. (2000).
54. Tom Huskinson, N. G. (2016). *Wellcome Trust.* Retrieved 11 1, 2018, from www.wellcome.ac.uk
55. *U.S. Department of Health & Human Services*. (2018). Retrieved from https://grants.nih.gov/policy/clinical-trials/definition.html
56. Union, E. (2008). Consolidated version of the Treaty on the Functioning of the European. *Official Journal C 326* .
57. *United Nations*. Retrieved October 01, 2018, from http://www.un.org/en/documents/udhr/
58. Voigt P., von dem Bussche A. (2017). *The EU General Data Protection Regulation (GDPR) A Practical Guide.* Switzerland: Springer International Publishing AG.